

IBM Tivoli Storage Manager for System Backup and
Recovery



Installation and User's Guide

Version 5 Release 6

IBM Tivoli Storage Manager for System Backup and
Recovery



Installation and User's Guide

Version 5 Release 6

Second Edition (April 2003)

This edition notice applies to the *IBM Tivoli Storage Manager for System Backup and Recovery Version 5 Release 6* (program number 5698-SYS) and to any subsequent releases until otherwise indicate in new editions or technical newsletters. This edition replaces GC32-9076-00. IBM Tivoli Storage Manager for System Backup and Recovery will be referred to as "SysBack" in certain text within this document.

The following paragraph does not apply to the United Kingdom or any country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS MANUAL "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of expressed or implied warranties in certain transactions; therefore, this statement may not apply to you.

This publication could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of this publication. IBM may make improvements and/or changes in the product(s) and/or program(s) described in this publication at any time.

Requests for copies of this publication and for technical information about IBM products should be made to your sales office or the IBM Branch Office serving your locality.

You feedback is important in helping to provide the most accurate and high quality information. If you have comments about this book or any other IBM Tivoli Storage Manager documentation, please see "Contacting Customer Support" on page ix.

IBM and AIX are registered trademarks of International Business Machines Corporation.

© Copyright International Business Machines Corporation 2002,2003. All rights reserved.

US Government Users Restricted Rights - Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

© Copyright International Business Machines Corporation 2002,2003. All rights reserved.

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

IBM Tivoli Storage Manager for System Backup and Recovery Overview vii

About This Book. ix

Who Should Read This Publication	ix
IBM Tivoli Storage Manager for System Backup and Recovery Documentation	ix
Conventions Used in This Book.	ix
Contacting Customer Support	ix

Chapter 1. Installation 1-1

System Requirements	1-1
Hardware Requirements	1-1
Software Requirements	1-1
Upgrading from System Backup and Recovery for AIX - SysBack	1-2
Procedure for Installation from CD-ROM	1-2
Accessing the Online Documentation	1-3

Chapter 2. SMIT Overview 2-1

Accessing the IBM Tivoli Storage Manager for System Backup and Recovery	2-1
How the SysBack Menus are Organized	2-2
Backup & Recovery Options	2-2
Configuration Options	2-2
Tape Drives	2-3
Utilities	2-4
Device Selector Screens	2-4
Backups to Disk Image Files	2-6
Backup, List, Verify and Restore Command Output Screen	2-7
SMIT Help Screens	2-9
SMIT Fastpaths	2-9
Obtaining Command Line Options from SMIT	2-9

Chapter 3. License Configuration 3-1

Chapter 4. Performing Backups. 4-1

Understanding Incremental Backups.	4-1
Understanding Pull Backups	4-3
Backing up the System (Installation Image)	4-3
Backing up Volume Groups	4-10
Backing up File systems	4-16
Backing up Logical Volumes	4-21
Backing up Files or Directories	4-25
Understanding Exclude List Processing on Backup Operations	4-30
Using SysBack with Fire Walls	4-30
Backup Return Code Processing	4-31
Unattended Backups Running in the Background	4-32

Chapter 5. Backups to CD or DVD. 5-1

Requirements	5-1
Software	5-1

Hardware.	5-1
Important Considerations	5-2
Space	5-2
Limitations	5-3
Media	5-3
Speed	5-3
Initiating the Backup	5-3
Initiating a Restore.	5-4
Boot and Installation	5-4
Command Syntax and SMIT Menus	5-6

Chapter 6. Offline Mirror Backups. 6-1

Purpose	6-1
Restrictions	6-1
Performing an Offline Mirror Backup	6-2
Maintaining Backup Command Files.	6-5
Maintenance Utilities	6-7
Synchronizing Stale Partitions	6-7
Recover from a Failed or Aborted Offline Mirror Backup.	6-10
Command Syntax and SMIT Menus	6-11
Manual Recovery	6-13

Chapter 7. Local User Access 7-1

Understanding Local User Access Permissions	7-1
Adding or Changing Local User Device/Directory Access.	7-2
Listing User Access	7-4
Removing User Access	7-4

Chapter 8. Remote Services 8-1

Understanding Remote Host and User Access Permissions	8-2
Backing Up, Listing, Verifying, or Restoring from Remote Backup Devices	8-4
Configure Remote Services	8-4
Adding or Changing Client Host Access to This Server	8-4
Listing Client Access	8-7
Removing Client Access	8-7
Adding or Changing the List of Remote Backup Servers	8-8
Listing Remote Backup Servers	8-10
Changing Remote Access Checking.	8-10
Removing a Remote Backup Server.	8-11
Remote Commands Access for use with Pull Backups	8-11
Configuring Remote Services in an NIS Environment	8-12

Chapter 9. Exclude Lists. 9-1

Adding a File, Directory or Logical Volume to an Exclude List	9-2
Listing Excluded Files or Directories.	9-4
Removing Files or Directories from an Exclude List	9-4

Deleting an Exclude List File	9-5
---	-----

Chapter 10. Recreating or Restoring from Backups 10-1

Removing Volume Groups, Logical Volumes, and Filesystems	10-1
Recreating Volume Groups, Logical Volumes, and Filesystems	10-2
Understanding Incremental Restores	10-7
Restoring Data from a Backup	10-8

Chapter 11. Changing the Volume Group, Logical Volume and Filesystem Attributes 11-1

Selecting Physical Volumes for Volume Groups	11-2
Change Physical Volume Attributes	11-4
Changing Volume Group Attributes	11-4
Selecting Physical Volumes for Logical Volumes	11-8
Changing Logical Volume Attributes	11-9
Changing Filesystem Attributes	11-16
Advance Install Options	11-20

Chapter 12. System Installation and Maintenance 12-1

Recovery Installation	12-1
No-prompt Installation	12-1
Handling Installation Errors	12-2
The SysBack Installation and Maintenance Menu	12-2
Changing the Installation Device	12-3
Changing Volume Group & Logical Volume Information	12-7
Installing the System with Current Settings	12-8
Utilities Menu	12-11
Rebooting the System Menu	12-18

Chapter 13. Network Boot/Installation Configuration 13-1

Classic Network Boot and NIM Resource Boot	13-1
Classic Boot	13-1
NIM Resource Boot	13-2
Classic Network Boot	13-2
Accessing and Configuring the Classic Network Boot Menus	13-2
Configuring or Updating a Network Boot Image	13-3
Adding or Changing a Network Boot Client	13-3
Setting the Network Install Client Defaults	13-5
Rebuilding Network Boot Images	13-9
Removing a Network Boot/Install Client	13-9
NIM Resource Boot	13-10
Accessing and Configuring the NIM Resource Menus	13-10
Installing SysBack into a SPOT Resource	13-10
Querying for SysBack Installation in SPOT Resource	13-12
Adding or Changing a Network Boot Client	13-12
Rebuilding Network Boot Images	13-13
Removing a Network Boot/Install Client	13-13
Initiating an SP Node Boot and Install	13-13

Chapter 14. RS/6000 Scalable POWERParallel Systems® (SP) Boot and Install Utilities 14-1

Advantages of the SysBack SP Boot and Installation Utilities	14-1
How SysBack works with NIM on the SP System	14-2
Special Assumptions	14-2
Accessing the SP Boot and Install Options	14-3
Completing the Initiate SP Node Boot and Install Menu	14-3
Unprompted and Prompted Installations	14-4
Troubleshooting Tips	14-4

Chapter 15. Integrating to IBM Tivoli Storage Manager 15-1

Prerequisites, Limitations, and Exclusions	15-1
Basic Setup and Configuration Tasks	15-2
Register a TSM Node	15-2
Install the API Client	15-2
Configure the TSM Client System Options File	15-2
Set TSM Environment Variables	15-3
Create the TSM Virtual Device	15-4
Additional Configuration for Bare Metal Recovery	15-4
Creating, Listing, Changing, and Removing the TSM Virtual Device for SysBack	15-4
Creating a TSM Virtual Device	15-4
Listing a TSM Virtual Device	15-6
Changing the TSM Virtual Device	15-7
Removing the TSM Virtual Device	15-9
Performing Backups to a TSM Server	15-11
Listing and Verifying Backups in a TSM Server	15-11
Querying Backups and TSM Management Classes	15-11
Querying Backups	15-11
Querying Current Management Class Bindings	15-15
Querying File Spaces on the TSM Server	15-16
Binding and Rebinding Backups to TSM Management Classes	15-17
Binding Backups	15-17
Rebinding Backups	15-18
Excluding Objects from Backups	15-18
Restoring Backups from a TSM Server	15-18
Configuring Network Boot Options for a TSM Bare Metal Recovery	15-18
Bare Metal Recovery and System Reinstallation from a TSM Server	15-21
Additional Information Resources	15-25
Using Multiple Backup and Restore Sessions	15-25
Problem Determination	15-26
The SysBack Command Output	15-26
The SysBack Activity Log	15-26
SysBack Error Log for the TSM API	15-26
Debug Options	15-27
Interoperability with System Backup and Recovery for AIX - SysBack Versions 5.1 - 5.4	15-27

Chapter 16. Utilities 16-1

Displaying SysBack Product Installation History	16-1
Printing or Displaying System Configuration	16-2

Creating a Bootable Tape (Without Data)	16-3
Creating a Bootable CD/DVD (Without Data)	16-5
Changing SysBack Tape Boot Defaults	16-9
Changing SysBack CD/DVD Boot Defaults	16-12
Changing the Read Permission on a Disk Image File	16-16
Creating or Editing an LVM Information File	16-18
Creating a Custom Installation Diskette	16-19
Changing SysBack Program Defaults	16-21
Backup Format Settings	16-22
End of Tape (EOT) Processing Options	16-23
Error Handling Settings	16-25
SysBack Network Settings	16-26
Logging	16-27

Chapter 17. Copying Backups to a New Media Type 17-1

Copy Backup from Disk Image or CD/DVD to Tape	17-1
Copy Backup Tape to Backup Disk Image	17-3
Copy Backup Tape to Backup Tape	17-5

Chapter 18. Listing or Verifying Backups 18-1

Listing Backup Contents	18-1
Verifying Files on System Backup	18-3

Chapter 19. Activity Logging 19-1

Accessing the SysBack Logging Menus	19-1
Changing the SysBack Logging Attributes (Size and Location)	19-1
Displaying the SysBack Log	19-2

Chapter 20. Scheduled Backups and Scripts 20-1

Scripts	20-1
Accessing the Backup Scripts Menu.	20-1
Creating a Backup Script File	20-1
Changing a Backup Script File	20-3
Removing a Backup Script File	20-4
Accessing the Backup Schedules Menus	20-4
Creating a Backup Schedule	20-5
Updating a Backup Schedule	20-6
Listing Backup Schedules	20-7
Removing a Backup Schedule.	20-7

Chapter 21. Virtual Devices 21-1

Types of Virtual Devices	21-2
Volume Numbering	21-2
Autoloaders	21-3
Adding a Virtual Device	21-3
Listing Virtual Devices	21-5
Removing a Virtual Device	21-5

Chapter 22. Tape Drives 22-1

Listing tape drives	22-1
Configuring a defined tape drive	22-2
Unconfiguring an Available Tape Drive	22-2
Changing Tape Drive Characteristics	22-2

Unloading or Ejecting a Tape from the Drive	22-3
---	------

Appendix A. Commands A-1

cfgremrootaccess	A-2
chimagefile	A-4
chinstclient	A-6
cfglocaccess	A-10
cfgremaccess	A-12
cfgremserver	A-15
cfgremsvs	A-17
cfgvirdev	A-18
chexcludelist	A-20
editlvminfo	A-22
getlvminfo	A-23
lscfginfo	A-27
mkdirback	A-29
mkjfsback	A-33
mklvback	A-37
mksbnetboot	A-41
mkvgback	A-45
mkvginfo	A-49
readsheader	A-53
remakevg	A-55
sblog	A-58
sbclient	A-59
sbcomp and sbuncomp.	A-62
sbcron	A-63
sbdevice	A-65
sbejecttape	A-67
sbeot	A-68
sbfwd	A-69
sbread	A-71
sbscript	A-74
sbspboot	A-76
sbspotcust	A-77
sbtsmdevice	A-79
sbtsmlist	A-81
sbtsmnetcfg	A-83
sbwrite	A-85
sysback	A-90
sysrestore	A-96

Appendix B. Booting a System for SysBack Installation or Maintenance . B-1

Initiating the boot process	B-1
Common Hardware Reference Platform (uni or multi-processor)	B-1
Microchannel-based RISC System/6000 (uniprocessor)	B-1
Microchannel-based RISC System/6000 SMP (multiprocessor)	B-2
PCI-based (RSPC) RISC System/6000 (uni or multi-processor)	B-3
Initiating the Network Boot.	B-4
Completing the Boot Process	B-4
Troubleshooting a Network Boot	B-5
Determining the Network Adapter Hardware Address	B-5

Appendix C. LEDs C-1

Appendix D. Creating Scripts for Customizing the System Backup and Install Process D-1

Script Names	D-1
Post-Installation Scripts	D-3
Sample Scripts	D-3

Appendix E. Device/System-Specific Information E-1

IBM 7208 8mm Tape Drives	E-1
IBM 3490, Magstar®, DLT and LTO Tape Drives	E-1
Other Tape Drives	E-2

IBM 7331 8mm Tape Library	E-2
IBM 7332 4mm Tape Library	E-3
Other Tape Libraries or Autoloaders.	E-3
IBM 7133 Serial Storage Architecture (SSA) disk subsystem	E-3
IBM 7135 RAIDiant Array	E-4
IBM 7137 and Other RAID Devices	E-4

Appendix F. Accessibility F-1

Appendix G. Notices G-1

Trademarks	G-3
----------------------	-----

IBM Tivoli Storage Manager for System Backup and Recovery Overview

IBM Tivoli Storage Manager for System Backup and Recovery (also known as “SysBack”) provides system administrators and other system users with a simple, efficient way to backup and recover data from a command line or a SMIT menu-driven interface. SysBack lets you recover all or part of the system. SysBack is also flexible; you can install one system installation image to another system with either identical or different hardware configurations, called “cloning”

SysBack features let you:

- Create various types of backups, including:
 - Full system (installation image)
 - Volume groups
 - Logical volumes (raw data)
 - Filesystems
 - Specific directories or files
- Incrementally backup and restore data.
- Perform “power” system backups that enable faster backup and restore times by backing up all data as raw logical volumes and heighten read/write performance while reducing CPU usage.
- Perform backups to locally attached tape drives or files on disk and remote hosts across the network.
- Selectively exclude specific files, directories, filesystems, or logical volumes from backups.
- Centrally manage backup clients using “pull” backups from a single server.
- Create backup scripts for easy automation.
- Define backup schedules for easy automation.
- Execute pre and post-backup scripts that enable environment-specific task automation, including halting database applications before beginning a backup.
- Perform backups to multiple sequential devices, automatically continuing the backup on the next device when the first is full and minimizing manual intervention when autoloading libraries are not available.
- Perform backups to multiple parallel devices, called “striping,” which lets you complete a single backup in a fraction of the normal time.
- Create multiple copies of a single backup to different devices in approximately the same time it takes for a single copy.
- View progress status indicators that display estimated backup or restore sizes, times, performance estimates and a completion percentage estimate.
- Receive completion status logs on all backup, list and verification operations.
- Use SMIT menus to configure SysBack options, which let you backup and restore volume groups, logical volumes, filesystems, directories, or files and list and verifying backup images.
- Use sequential autoloading devices to minimize manual intervention and tape loading operations.
- “Stack” multiple backups on a single tape for all backup types.

- Reinstall the system to its original device configuration, including the volume group and logical volume placement on disk and attached devices, using Full System (Installation) Image to the same or different system (also called “cloning”).
- Install the system from local boot/installation media or from a TSM server.
- Perform a network boot or installation to alleviate the need for local boot or installation media using SysBack functions or existing Network Installation Manager (NIM) resources.
- Perform Recovery Installation that restores only the base operating system (root and /usr filesystems) without affecting other data in the rootvg or other volume groups.
- Preserve multi-copied (mirrored) or striped logical volumes on recreate.
- Import, ignore, or recreate/restore each volume group or logical volume from a single backup media during installation.
- Retain exact partition placement of logical volumes or make contiguous partitions of any that have become fragmented; this will improve I/O performance on recreate.
- Execute post-installation scripts to perform environment specific tasks.
- Use post-installation to remove SysBack or network configuration after cloning a backup image to a different machine or to indicate the location of installation media for automatically installing device support to the new machine.
- Set network and tape boot defaults to minimize, and often eliminate, the need for user prompting during an installation.
- Edit or change the physical location and attributes of volume groups, logical volumes, and filesystems during recreation.
- Restore data at the volume group, logical volume, filesystem, directory or file level.
- Interactively select files to restore by letting you specify a filelist, use a search word or use a wildcard to narrow the list.
- Exclude select filesystems or logical volumes during restore operations.

About This Book

This book contains information on configuring and using IBM Tivoli Storage Manager for System Backup and Recovery (also known as “SysBack”). The book contains instructions on using the System Management Interface Tool (SMIT) menus for performing backups as well as a commands reference to perform SysBack functions without the SMIT menus.

Who Should Read This Publication

This book is intended for system administrators responsible for managing the AIX® operating system on RS/6000® or pSeries™ systems. Readers of this book are expected to have a basic understanding of the SMIT menus and have already configured devices for backing up the operating system. Readers should also be familiar with the general layout of the AIX system, including an understanding of the volume groups, logical volumes, and filesystems.

IBM Tivoli Storage Manager for System Backup and Recovery Documentation

IBM posts publications for this and all other Tivoli products, as they become available and whenever they are updated, to the Tivoli Information Center Web site. You can access updated publications in the Tivoli Information Center from the following Customer Support for Tivoli products Web site:

<http://publib.boulder.ibm.com/tividd/td/tdprodlist.html>

Conventions Used in This Book

The following highlighting conventions are used in this book:

Bold	Identifies command, keywords, files, directories, and other items whose names are predefined by the system.
<i>Italics</i>	Used for emphasis and to identify parameters whose actual names or values are to be supplied by the user.
Monospace	Identifies examples of specific data values, text similar to what you might see displayed, messages from the system, or information you should actually type.

Contacting Customer Support

For support of this or any Tivoli product, you can contact Tivoli Customer Support in one of the following ways:

- Visit the Storage Manager technical support Web Site at:
<http://www.ibm.com/software/sysmgt/products/support/>
- Submit a problem management report record (PMR) electronically at IBMSERV/IBMLINK. You can access IBMLINK at:
<http://www2.ibm.link.ibm.com>
- Submit a problem management record (PMR) electronically at:
<http://www.ibm.com/software/support/probsub.html>
- Customers in the United States can also call 1-800-IBM-SERV.

- International customers should consult the web site for customer support telephone numbers.
- You can also review the IBM Software Support Guide which is available on our web site at: <http://techsupport.services.ibm.com/guides/handbook.html>

Chapter 1. Installation

To install IBM® Tivoli® Storage Manager for System Backup and Recovery, also known as, SysBack™, you must have the prerequisite software installed on your system.

System Requirements

Hardware Requirements

SysBack supports the following hardware:

- IBM @server pSeries™ and RS/6000® systems, including RS/6000 SP™ environments, and systems capable of the logical partitioning of AIX®.
- @server pSeries Cluster 1600 systems using the PSSP option

Software Requirements

The following software is required to use SysBack:

- AIX V4.3.0 or later, AIX 5L V5.1, or V5.2
- If you will be using the **TSM Integration** feature, you will also need:
 - A previously configured TSM server must be at level 5.1.5 or higher.
 - The 32-bit TSM API client must be installed and at level 5.1.5 or higher
 - The TSM node name used for SysBack backups must be registered on the TSM server and configured to use the passwordaccess generate option.

Note: This feature is not available in SysBack versions less than 5.6.

- The **bos.sysmgmt.sysbr** fileset.
- If you will be using the **Remote Services** functions of SysBack, install the following:
 - bos.rte.net
 - bos.net.tcp.client
- If you will be using the **Classic Network Boot** functions for the Network Installs, install **bos.net.nfs.client**
- If you will be using the **NIM Resource Network Boot** functions for Network Installs, the NIM environment and resources must first be installed and configured in the desired locations for SysBack to use these resources. For information on installing and configuring NIM, see the book, *Network Installation Management Guide and Reference*
- If you will be using SysBack on **SP or Cluster 1600 systems**, you must be using PSSP level 3.4 or 3.5.

Note: At this time, SysBack does not include support for @server pSeries Cluster1600 systems using the CSM option available in AIX 5.2.

- When AIX is installed, the following are installed automatically with the system and may not be removed in order for SysBack to function properly:
 - bos.rte.bosinst
 - bos.rte.archive
 - bos.rte.libnetsvc (when using Network Install functions)

- If you will be using the **CD / DVD backup** feature, please refer to Chapter 5, “Backups to CD or DVD”, on page 5-1 for additional requirements specific to this feature.

Upgrading from System Backup and Recovery for AIX - SysBack

If you are upgrading from System Backup and Recovery for AIX - SysBack™ versions 5.1.x, 5.2.x, 5.3.x, or 5.4.x, you will not need to uninstall it before installing the IBM Tivoli Storage Manager for System Backup and Recovery (SysBack) version 5.5 or 5.6 product.

The installation process for IBM Tivoli Storage Manager for System Backup and Recovery will preserve any previous configurations, as well as, to automatically make the **sysback.rte** fileset obsolete.

Procedure for Installation from CD-ROM

After the prerequisite software is installed:

1. Log in as a root user. You will see the following:

```
IBM AIX Operating System
(c) Copyright IBM Corp. 19XX, 19XX
(/dev/console)
login: root
```

2. Insert the *IBM Tivoli Storage Manager for System Backup and Recovery* installation CD into the CD-ROM drive.
3. Type the AIX command `smitty install`.

Note: This command invokes the System Management Interface Tool (SMIT), which presents a menu-driven environment for the installation process. The argument `install` is a fastpath that takes you directly to the software installation process. The menu selections differ from one version and release of the operating system to another, so menu selections displayed on your system may differ slightly.

4. From the Software Installation and Maintenance menu, select **Install and Update Software**.
5. Select **Install and Update from the LATEST Available Software**.
6. At the INPUT device/directory for software prompt, type the device name of the CD-ROM drive. For example, `/dev/cd0`.
7. The following screen is displayed:

Install and Update from LATEST Available Software

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

	[Entry Fields]	
* INPUT device/directory for software	/dev/cd0	
* SOFTWARE to install	[_all_latest]	+
PREVIEW only? (install operation will NOT occur)	no	+
COMMIT software updates?	yes	+
SAVE replaced files?	no	+
AUTOMATICALLY install requisite software?	yes	+
EXTEND file systems if space needed?	yes	+
OVERWRITE same or newer versions?	no	+
VERIFY install and check file sizes?	no	+
Include corresponding LANGUAGE filesets?	yes	+
DETAILED output?	no	+
Process multiple volumes?	yes	+

F1=Help
F5=Reset
F9=Shell

F2=Refresh
F6=Command
F10=Exit

F3=Cancel
F7=Edit
Enter=Do

F4=List
F8=Image

Figure 1-1. The Install and Update from Latest Available Software Menu

8. To install the SysBack product, accept the default settings.
To install individual filesets, highlight **Software to install** and press F4. Individually, select the filesets to install.

Notes:

- a. The SysBack 5.5 and 5.6 product fileset is: **tivoli.tsm.client.sysback.rte**
- b. The SysBack 5.5 and 5.6 license filesets are:
tivoli.tsm.client.sysback.license.rte and
tivoli.tsm.client.sysback.license.cert
- c. The SysBack 5.1 - 5.4 product fileset is: **sysback.rte**
- d. Licensing for SysBack 5.1 - 5.4 is key specific. Please refer to
<http://sysback.services.ibm.com/> or other documentation that
accompanied your order.
- e. The SysBack HTML version of the manual is no longer available as the
fileset **sysback.html.en_US**. To view the manual in HTML form, please
refer to <http://publib.boulder.ibm.com/tividd/td/tdprodlist.html>
9. Press Enter to confirm selections and install the software.
10. On AIX 5.1 systems, you will be prompted to “accept” the electronic license
agreement. Indicating a “No” response will prohibit the installation of these
filesets.

Accessing the Online Documentation

IBM posts publications for this and all other Tivoli products, as they become available and whenever they are updated, to the Tivoli Information Center Web Site. You can access updated publications in the Tivoli Information Center from the following Customer Support for Tivoli products web site:
<http://publib.boulder.ibm.com/tividd/td/tdprodlist.html>

Chapter 2. SMIT Overview

This chapter provides information about the SMIT menu interface. SMIT is used for virtually all AIX system administrative tasks.

Accessing the IBM Tivoli Storage Manager for System Backup and Recovery

To access the System Backup & Recovery for AIX menus, type `smit` to access the System Management Interface Tool. After SysBack is installed, IBM Tivoli Storage Manager for System Backup and Recovery is displayed at the bottom of the main menu. Select this option to access additional SysBack screens. You can alternatively type `smit sysback` to jump directly to the SysBack screens. The following is an example of the SysBack Main SMIT Menu as shown using the ASCII SMIT menu.

```
IBM Tivoli Storage Manager for System Backup and Recovery

Move cursor to desired item and press Enter.

Backup & Recovery Options
Configuration Options
Tape Drives
Utilities
Backup Schedules and Scripts

F1=Help      F2=Refresh   F3=Cancel    F8=Image
F9=Shell     F10=Exit     Enter=Do
```

Figure 2-1. ASCII version of the SysBack Main SMIT Menu

The ASCII SMIT menu is displayed by default if AIXwindows is not running. If AIXwindows is running, and SMIT is started from the desktop or from an aixterm window, the graphical version of SMIT (*msmit*) is displayed by default. The remainder of the screens displayed in this section use the ASCII SMIT format.

Note: To use most of the options within the SysBack menus, log in to the system as a root user. This is for several reasons:

1. Only a root user has authority to read, and therefore backup or restore, many files in the system.
2. When restoring files under a non-root user, that user, if permitted to read the files, becomes the new owner of the files. Files are returned to their original ownership only when restored by a root user.
3. Many options, such as changing the block size of the tape drive, creating network boot images, or configuring network server and client options, require that you have root privileges to perform the task.

How the SysBack Menus are Organized

The menus are organized by the type of backups that you can perform, followed by additional options used for configuring or customizing additional SysBack options. The SysBack Main Menu includes the following options:

Backup & Recovery Options

Use this option to display additional options for backing up, listing, verifying, or restoring files from a backup depending on the type of backup performed. It is not necessary to know the backup type to perform any of the list, verify, recreate or restore options, as the system will read the backup to determine the backup type, and presents only additional options that are relevant to that type of backup.

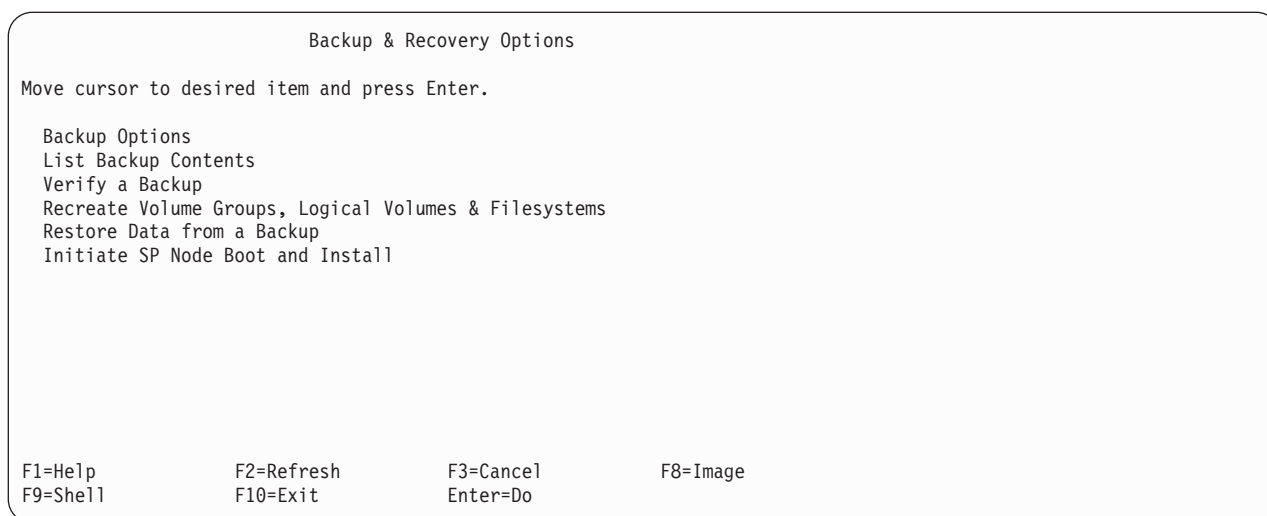


Figure 2-2. Backup & Recovery Options

Use **Backup Options** to create a backup of the system that can be used to reinstall the system from a system failure, or to use the backup to install other systems. Additional options available from the Backup Options menu enable you to back up a smaller part of the system or only specific files or directories.

Configuration Options

This menu provides additional options for configuration tasks, such as providing access to local and remote users, adding and deleting entries from exclude lists, and creating or deleting virtual device descriptions. The this menu is displayed below:

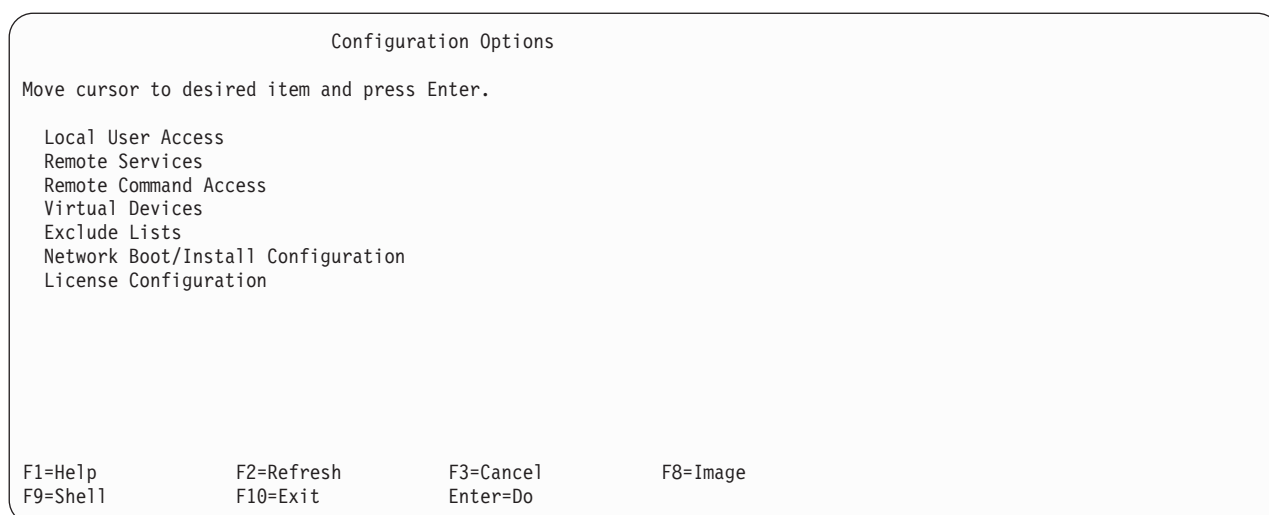


Figure 2-3. Configuration Options

The following options are available on this menu:

Local User Access

Provides backup permission to specific or all users on the system. You can also indicate which local tape drives or virtual devices the users are allowed to access and the directories to which they are allowed to save backup images.

Remote Services

Provides backup access from remote systems to local devices or directories. You can indicate which users on the remote hosts are allowed access and the specific devices or directories to which they are allowed to backup.

This option is also used on the client system to indicate which servers to which they want to backup. Only servers that have granted access to the client can be configured on the client.

Virtual Devices

Adds, lists, and removes virtual devices. Virtual devices are logical device names assigned to one or more physical devices, providing a simpler way to back up to multiple devices or autoloaders.

Exclude Lists

Enters, lists, or deletes entries from an *exclude file*. The exclude file contains names of individual files or directories to exclude from all backups generated by SysBack.

Network Boot Configuration

Creates network boot images that enable client machines to be booted from the network, therefore requiring no local boot media.

Tape Drives

Use this option to change the physical block size of tape drives or enable or disable tape drives on the system. This is particularly useful when you want to temporarily disable client machines from accessing the tape drives. An additional option enables you to unload or eject a tape cartridge from a tape drive or tape autoloader. The menu is displayed below:

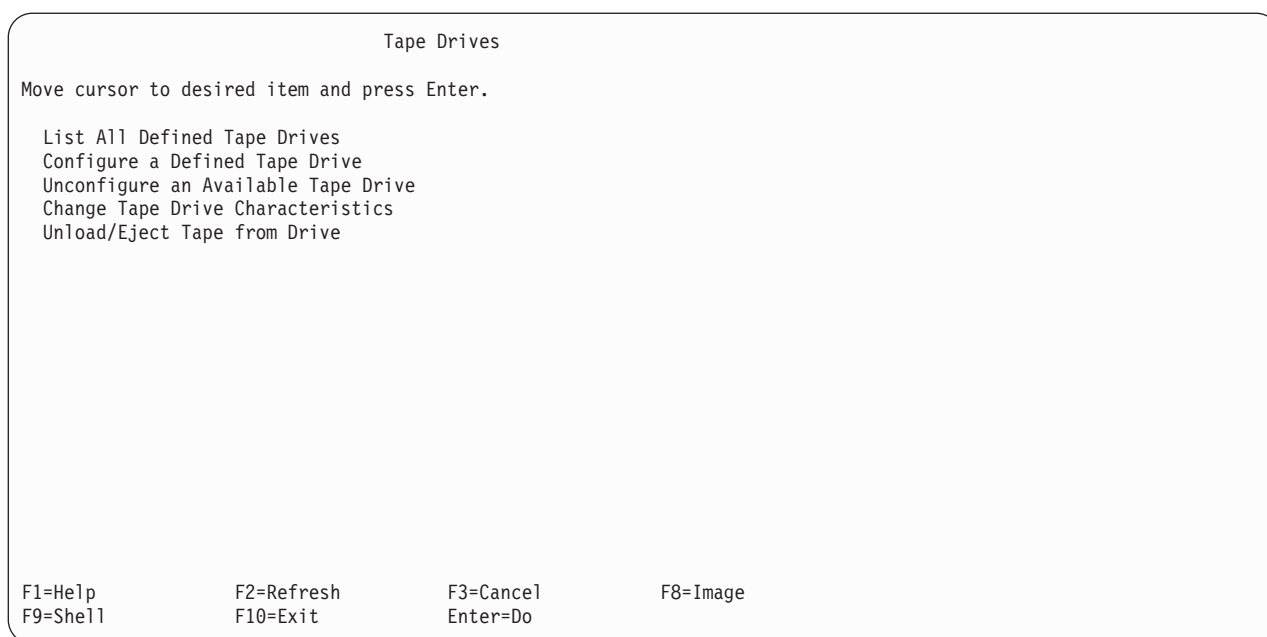


Figure 2-4. Tape Drives

Utilities

This menu provides a list of miscellaneous options. The options on this menu might differ depending on your level of AIX installed and might change as new options are added to SysBack.

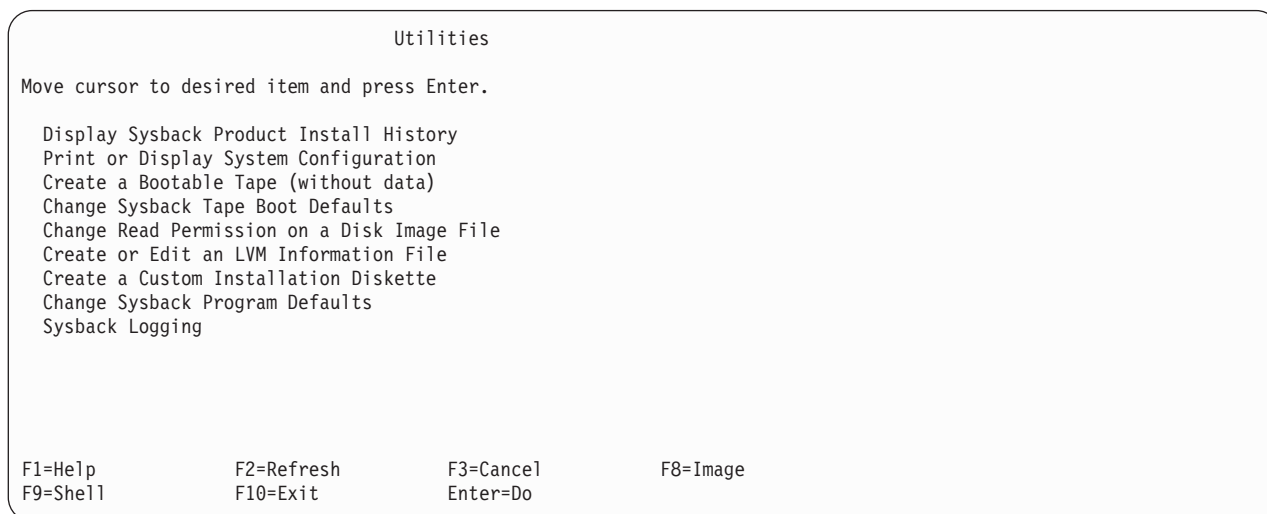


Figure 2-5. Utilities

Device Selector Screens

When selecting a backup, list, verify, recreate or restore option from any SMIT menu, you are prompted for the device, directory, or filename to use.

Various tape devices, virtual devices, or filename options are displayed, depending on the backup permission granted the specific user or host. When you back up to a local device or directory, the backup options are determined by the local access, as defined using the **Add or Change Device/Directory access to Local Users** option.

When you back up to a remote backup server, the backup options are determined by the **Add or Change Client Host Access to this Server** option executed on the server. If no directories are defined for disk image file backups, then no disk file options are provided.

Figure 2-6 shows the backup options that might be included on the SMIT menu:

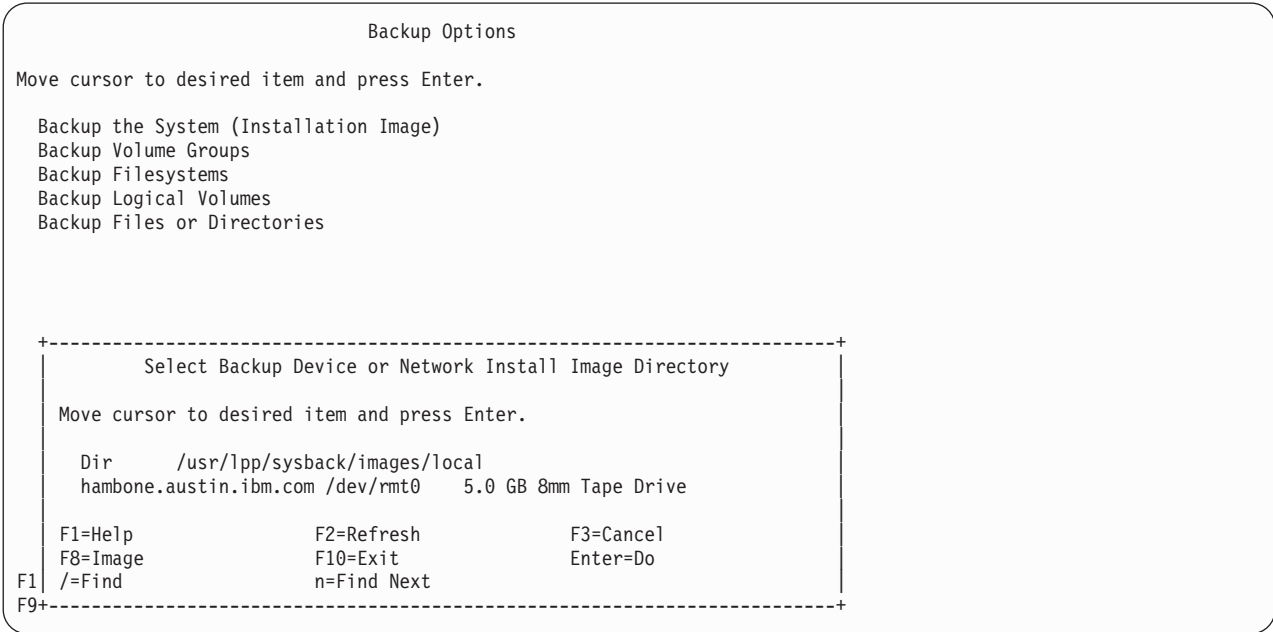


Figure 2-6. Backup Options

The first column contains the device type and can be any of the following:

- | | |
|------------------|--|
| VirDev | Virtual devices that you have configured. The device name (vdev0) is automatically assigned by the system. The description shown is either one that you assign or a default description assigned by the system. The physical devices that make up the virtual device are listed at the end of the line in parentheses. |
| Tape | Tape drives available on the local system. Local tape drives are always displayed first in the list. |
| Dskt | Diskette drives on the local system. A diskette option is not displayed for a system backup. |
| Dir | For backup options, a directory name, if the user has permission to back up to a disk file. The directory shown is the directory or directories specified when backup permission was enabled for the user. For list, verify, and restore options, all files in the user's backup directories are displayed. |
| File | For list, verify, recreate and restore options, the name of a local disk image file. Only files in the directories the user has access to are displayed. Files of all backup types are shown. |
| Hostname: | A remote option. The hostname is the name of a server for which this host has remote access. The information can be any one of the following: |

Tape Drive Name

Tape drives on the remote machine. Only remote tape drives on hosts that have granted access to this host, as well as those that have been defined by the local host, are included on this selector screen.

Virtual Device Name

Virtual devices configured on the server. The virtual device description from the remote machine and the physical tape drive name(s) are shown. Only virtual devices for hosts that have granted access to this host, as well as those that have been defined by the local host, are included on this selector screen.

File or Directory

For list, verify, recreate and restore options, a filename is shown for each disk image backup file that exists on the server in the directories for which this host has access. For backup options, a directory name is shown for all directories this host has permission to write to.

You must select one of the options provided on the selector screen before proceeding. After you select an option, you can change the device, filename or unique ID selected on the dialog screen that follows, but the backup cannot execute unless you have permission to access the specified device or directory.

Backups to Disk Image Files

To perform a disk file backup, select a directory name from the device selector screen. A filename is automatically generated as follows:

/Directory/Type.Hostname.UniqueID

The filename contains the following parts:

Directory	The directory selected.
Type	The type of backup to be performed. One of the following is used: SB System Backup VG Volume group LV Logical Volume FS Filesystem FD File/Directory
Period (.)	Delimiter.
Hostname	The name of the host performing the backup. This is set to "localhost" if no hostname is defined.
Period (.)	Delimiter.
UniqueID	A unique ID that, by default, contains the date and time of the backup in "MMDDhhmm" format. For example, if a backup is made on Feb. 28 at 3:20 P.M., the unique ID would be "02281520".

You can later change this ID to any other value that might more accurately describe the backup contents.

Although the filename in SMIT is displayed only as shown above, most backups actually create more than one file, each named as above, but with an additional extension. The first file has a **".TOC"** extension, indicating the file is the table of contents of the backup. For a File/Directory backup, the **".TOC"** file also contains the backup data, because there is always only one image in this backup. For all other backup types, an additional file is created for each logical volume or filesystem included in the backup, with the logical volume name as the file extension. This file contains the actual backup data for each logical volume or filesystem.

Backup, List, Verify and Restore Command Output Screen

The output screen for the backup, list, verify, and restore options is different from that of other SMIT-executed commands. This screen provides the following advantages:

- Output is not saved in the SMIT log file (**smit.log**). This prevents very long file lists from taking unnecessary space on the disk. You are still provided the option of writing the output to a log file after the command has completed.
- There is no delay when the command has completed. The delay is normally required for SMIT processing and writing of the **smit.log** file.
- Command output (stdout) and error (stderr) are displayed in separate windows. This provides much cleaner output for commands that provide both standard output and standard error messages.
- The complete command and the time the command started and ended is displayed at the top of the screen.

The following is an example of the output of a file/directory backup executed from SMIT:

```
COMMAND: mkdirback -hhambone.austin.ibm.com -f/sysback.images/fatrat/backu ...
STARTED: Feb 28 18:37:36   ENDED:                                     STATUS: Running
                                     Command Output
Generating file list ..
```

Command Error / Status

```
NOTE: Estimated megabytes is approximate since data is compressed.
Backing up Files "/tivol1"
Start date is Mon Feb 28 18:36:31 2000
User is root at fatrat
Estimated size is 678 MB
```

ESTIMATED PROGRESS			
% Complete	Elapsed Time	Megabytes	Kbytes/Sec
1	0 minutes of 42	7 of 678	272

Figure 2-7. The output of a file/directory executed from SMIT

Note that the screen is separated into two "windows." The first is for Command Output (stdout). The second is for Command Error (stderr) and Status. The

Command Error section is always used to display error messages but is also often used for other output, such as file lists, status indicators, and so on.

In the above example, a file/directory backup of the **/home/data** directory was performed. The user selected the **progress indicator** report output type during the backup, rather than the list of files. The progress indicator shows the estimated time and amount of data to be backed up, the actual percent, time, and amount complete, and the average performance in kilobytes per second.

When the command has completed, you can perform the following functions by pressing the appropriate function key:

F1 Help	Displays a help screen that provides details of the functions you can perform from this output screen.												
F2 Refresh	Erases and redisplay all the information you see. This is necessary only if there are other commands, such as system console information, running that output to this terminal and overwrite the command output.												
F3 Return	Returns to the previous SMIT dialog screen.												
F4 Select	<p>Toggles between the Command Output and the Command Error/Status window, enabling each to scroll independently. The active window is indicated by the arrows (====> <i>window</i><====).</p> <p>After you have selected the window to scroll, you can then move through the output using the following keys:</p> <table><tr><td>Page Down</td><td>Scroll forward one screen</td></tr><tr><td>Page Up</td><td>Scroll backward one screen</td></tr><tr><td>Down—Arrow/Enter</td><td>Scroll backward one line</td></tr><tr><td>Up—Arrow</td><td>Scroll back one line</td></tr><tr><td>Home</td><td>Display first screen</td></tr><tr><td>End</td><td>Display last screen</td></tr></table>	Page Down	Scroll forward one screen	Page Up	Scroll backward one screen	Down—Arrow/Enter	Scroll backward one line	Up—Arrow	Scroll back one line	Home	Display first screen	End	Display last screen
Page Down	Scroll forward one screen												
Page Up	Scroll backward one screen												
Down—Arrow/Enter	Scroll backward one line												
Up—Arrow	Scroll back one line												
Home	Display first screen												
End	Display last screen												
F5 Save	<p>Save the entire output in a log file. You are asked to enter the name of the log file. The default file is \$HOME/sysback.log, where \$HOME is the user's home directory. Either enter a new file name or press Enter to accept the default. The following example shows a sample output file:</p> <pre>COMMAND: mkdirback -f/dev/rmt1 -s /home/tj START TIME: Mar 20 02:22:30 END TIME: Mar 20 02:25:49 STATUS: Successful ===== Command Output ===== Rewinding rmt1 ... Generating file list .. File/Directory backup completed successfully. ===== Command Output ===== Backing up Files */home/tj* Start date is Thu Mar 20 02:22:33 1997 User is root at sysdev41 Estimated size is 169 MB</pre>												

ESTIMATED PROGRESS

% Complete	Elapsed Time	Megabytes	Kbytes/Sec
100	3 minutes of 3	170 of 170	913

Backup ended Thu Mar 20 02:25:46 1997
170 megabytes written to 1 volume.

SMIT Help Screens

You can obtain help information from any point within SMIT. If a menu selection is currently displayed, highlight a function and press F1 for information regarding the use of that function. For any dialog selection, F1 provides information on the use of that selection, the options available, and how they affect the function being performed.

SMIT Fastpaths

From any SMIT menu or dialog screen (where you type or change options), press F8 to display the SMIT *fastpath* for quickly reaching that selection from the command line. Later, to skip directly to the desired selection, you can type `smit fastpath` at the command line, where *fastpath* is the fastpath for the desired selection.

Obtaining Command Line Options from SMIT

You can execute any SMIT command outside of SMIT by placing the command in a shell script. You can place multiple commands in shell scripts to be executed in sequence, enabling a sequence of multiple commands to be performed without user interaction. You can also place the shell scripts in **cron**, an AIX job scheduling facility.

To obtain the command line options for a SMIT command, use the following steps:

1. Select the SMIT option to perform and any additional selections required for this function.
2. Fill out any fields or change the field values in the dialog screen as you would when executing the command from SMIT.
3. Before pressing Enter to execute the command from SMIT, press F6 to show the command on the screen.

The following is an example of the SMIT output when you press F6:

Backup Files or Directories

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

Hostname of server Device name Report output type	<div style="text-align: right; font-size: small;">[Entry Fields]</div> hambone.austin.ibm.com /dev/rmt0 progress indicator
---	--

SHOW COMMAND STRING

Press Enter or Cancel to return to the application.

* # Ignore "/usr/sbin/sbsmitout -sN" prefix
 # when executing outside of SMIT:

/usr/sbin/sbsmitout -s7 mkdirback -h'hambone.austin.ibm.com' -f'/dev/rmt0' '-x' '/home'

F1 F1=Help	F2=Refresh	F3=Cancel
F5 F8=Image	F10=Exit	Enter=Do

Figure 2-8. Results of Using the F6 Key to Show the Command String

Single quotes (') around text are required only when there is more than one word to a single command argument. They do not need to be used to surround a single word.

Backup, list, verify and restore commands contain the comment indicating that the prefix of the command **/usr/sbin/sbsmitout -sN** should be omitted. This prefix causes the command to be executed within the two-part SysBack SMIT command output screen previously described. Do not use this output screen should when executing commands at the command line if the intention is to not require user interaction.

Chapter 3. License Configuration

To license your IBM Tivoli Storage Manager for System Backup and Recovery (SysBack) software, you must simply install the:

- `tivoli.tsm.client.sysback.license.rte`
- `tivoli.tsm.client.sysback.license.cert`

filesets included on your product media in addition to the installation of the base `tivoli.tsm.client.sysback.rte` fileset.

Special licensing measures apply for customers using SysBack versions 5.1 - 5.4. There are no license filesets for this version of SysBack. For detailed information related to licensing your product, please refer to your product README file located at: `/usr/lpp/sysback/README.txt`, <http://sysback.services.ibm.com>, or other documentation that accompanied your order.

Chapter 4. Performing Backups

As soon as SysBack is installed, you can perform a backup to any local device or to the default SysBack backup image files directories.

To access the Backup Options:

1. At a command line, type `smit`.
2. Select **IBM Tivoli Storage Manager for System Backup and Recovery**.
3. Select **Backup & Recovery Options**.

You can also access this menu using the fastpath. To do this, type `smit sb_backup` at a command line. The following screen is displayed:

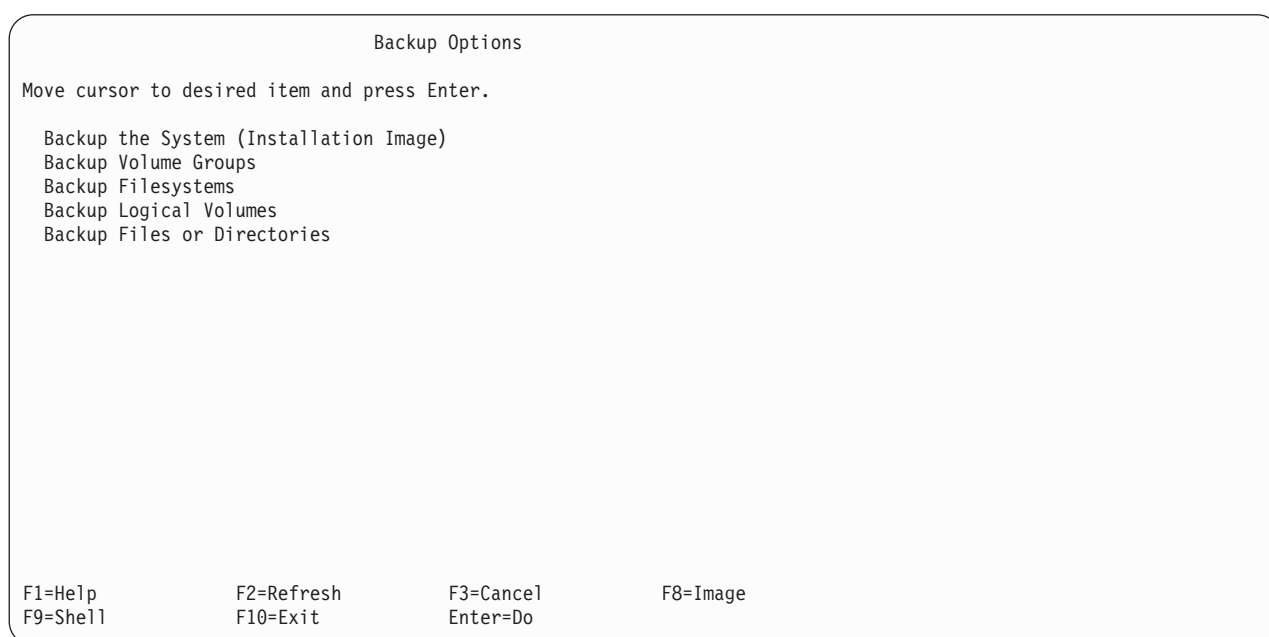


Figure 4-1. Backup Options

You can select any of the backup options, each of which are described in detail in this chapter. The first option, **Backup the System (Installation Image)**, is used to create a backup of the operating system and any additionally selected volume groups. This is the only backup from which the system can be reinstalled after an operating system failure. All other backups options back up smaller increments of data, such as volume groups or select file systems.

Understanding Incremental Backups

Incremental backups make it possible to back up only data that has changed since a prior backup, significantly reducing the backup time and media usage. Incremental backups can be performed for both volume group and file system backups.

You perform an incremental backup by indicating an incremental backup level. This level indicates that only files that have changed since the most recent previous

level should be included in the backup. Specifying level 0 indicates that all files should be backed up. Level 0 is still considered an incremental level; it is the base for all incremental levels that follow.

Any number of incremental levels from 0 through 9 can be used, but using too many levels can complicate the restore process.

Consider the following incremental backup examples:

Incremental backup of a file system is performed as follows:

Monday	level 0
Tuesday	level 1
Wednesday	level 2
Thursday	level 3
Friday	level 4
Saturday	level 5
Sunday	level 6

In this case, if you need to restore the entire file system from the backup performed on Sunday, you must restore every single backup from 0 through 6 in order to incrementally reapply the changes to date. Always restore level 0 first (when restoring from scratch) because only level 0 contains a backup of the entire file system. Then, in the correct sequence, reapply each level that follows, adding, replacing, and removing files until the file systems return to their most recent state.

Incremental backup of all volume groups, except the rootvg group, is performed as follows:

1st of month	level 0
every Friday	level 4
Monday-Thursday	level 7

In this example, a volume group backup is performed on the first day of the month. Every Friday a level 4 is performed, and every other day of the week (excluding Saturday and Sunday) a level 7 is performed. Because only three levels are used, no more than three backups need to be restored. If you need to restore the entire volume group because of failure, the restore sequence would be:

1. Restore level 0.
2. Restore the most recent level 4 if a level 4 was performed since the last level 0.
3. Restore the most recent level 7 if a level 7 was performed since the last level 4 or level 0.

Note: Use care when combining both volume group and file system incremental backups. An incremental volume group backup is identical to performing an incremental backup of each individual logical volume and file system in the volume group. Therefore, after performing a volume group level 0 backup, you can perform other incremental backup levels for specific file systems. If a level 0 backup of a file system is performed after a level 0 of the volume group containing that file system, any higher-level incremental levels for that file system are applied to the *most recent* (file system) backup.

For volume group incremental backups, an entire logical volume is included if any part of the logical volume has changed. If no data in the logical volume had changed, the logical volume is not included in the backup.

Understanding Pull Backups

Pull Backups help you centrally manage your backups by enabling you to initiate, and thereby control, backup operations from a single location. You can further automate this central management of backups using the SysBack Scheduling and Scripting functions described in Chapter 20, “Scheduled Backups and Scripts”, on page 20-1.

The machine that “pulls” the backup is called the “initiator” while the machine that is backed up is called the “backup system”. The machine that receives that backup data is called the “destination system”.

Pull backup enablement requires, not only Remote Services configuration, but also Remote Command Access configuration. The Remote Services configuration enables the data to be sent across the network from the backup system to the data destination machine. The Remote Command Access configuration enables the initiator system to pull the backups from the backup system.

Pull Backups can be done in a two-way or three-way manner. When the initiator system is also the data destination system, this is a two-way backup. When the initiator system is a different machine than the data destination system, and different than the backup system, this is a three-way backup.

Note that for three-way backups, Remote Services must be configured between Machine A, the backup system, and Machine B, the data destination. Remote Command Access must be also configured between Machine A, the backup system, and Machine C, the backup initiator. For more information on configuring Remote Services and Remote Command Access, see Chapter 8, “Remote Services”, on page 8-1.

The following SysBack backup options are discussed in this chapter:

- Backing up the System (Installation Image)
- Backing up Volume Groups
- Backing up File systems
- Backing up Logical Volumes
- Backing up Files or Directories

Backing up the System (Installation Image)

A system backup can be used in the following ways:

- To reinstall the entire system to its original state.
- To recreate or restore specific volume groups, file systems, or both on an already active system.
- To install a system backup created on one machine onto another machine with a different processor, platform type, or other system devices. This is called *cloning*. However, the machine being backed up must have installed all of the device support for the destination platform type, processor type and other required devices.

To back up the entire system:

1. From the Backup & Recovery Options menu, select **Backup the System (Installation Image)**.
Notes:
 - a. You must be logged in to the system as a root user.
 - b. At a command line, type `smit sb_sysback`.
2. If there are volume groups on the system other than `rootvg`, select the volume groups to include in the backup. From the list of volume groups, either select **none (rootvg only)** or highlight each additional volume group to include and press F7. Press Enter to continue.
3. On the Device Selector screen, highlight the device you want to use and press Enter.
4. One of the following screens is displayed. These screens show the default options and values available when you back up to either a local tape drive or a disk image file.

Backup the System

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

	[Entry Fields]	
Hostname of server	hambone.austin.ibm.com	
Device name	/dev/rmt0	
Create a Power Backup?	no	+
Report output type	progress indicator	+
Platform/kernel type for tape boot image	[rspc]	+
Network install support to include	<input type="checkbox"/>	+
Include non-JFS logical volumes?	yes	+
Rewind tape before starting backup?	yes	+
Forward to End of Tape before Starting Backup	no	+
Compress data before writing to media?	no	+
User description	<input type="checkbox"/>	
Buffer size (in Kbytes)	[64]	+#
Preserve physical partition mapping?	no	+
Device name for remote volume prompt	<input type="checkbox"/>	
Non-rootvg Volume Groups to include	<input type="checkbox"/>	+
[MORE]		

F1=Help

F5=Reset

F9=Shell

F2=Refresh

F6=Command

F10=Exit

F3=Cancel

F7=Edit

Enter=Do

F4=List

F8=Image

Figure 4-2. Default Options Available for Backing Up to Tape

Backup the System

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

	[Entry Fields]	
Backup Data Hostname	hambone.austin.ibm.com	
Images directory	/sysback.images/fatrat>	
Create a Power Backup?	no	+
* Backup file ID	[03061826]	
Dynamically Created Backup File ID	no	+
Report output type	progress indicator	+
Include non-JFS logical volumes?	yes	+
Compress data before writing to media?	yes	+
User description	[]	
Host read permission	all hosts	+
User read permission	all users	+
Buffer size (in Kbytes)	[64]	+#
Preserve physical partition mapping?	no	+
Overwrite existing backup with same ID?	no	+
Non-rootvg Volume Groups to include	[]	+
[MORE]		

F1=Help

F2=Refresh

F3=Cancel

F4=List

F5=Reset

F6=Command

F7=Edit

F8=Image

F9=Shell

F10=Exit

Enter=Do

Figure 4-3. Default Options Available for Backing Up to Disk Image File

The fields have the following definitions:

Backup Data Hostname

The hostname of the data destination system on which the selected backup device or file exists. You may edit this field as necessary to specify a the hostname of a remote system not listed in the device selector dialog screen. This is useful when initiating a Pull Backup.

Device name The device, if a tape drive or virtual device was selected. You may edit this field as necessary to specify a device on a remote system not listed in the device selector dialog screen. This is useful when initiating a Pull Backup.

Images directory

The directory name, if previously selected. You cannot change this field from this screen.

Create a Power Backup?

Default=no. Use Tab to change this field to “yes” if you want this backup to be a “Power” backup. A Power backup backs up all file systems as “raw” logical volumes, which usually provides much better backup and restore performance, but imposes the following limitations:

- You can restore only raw logical volumes from this backup. Therefore, when choosing to restore data from the backup, you will be allowed to restore only an entire logical volume and only if it is inactive. Because of this, you cannot restore any individual files or directories, only entire file systems; and no file systems, such as /, /usr and /var can be restored since they are always active.
- Because all file systems are backed up as raw logical volumes, the entire logical volume is backed up even if only

one-fourth of the file system is used. If this were the case with all file systems, the backup and installation would likely take longer than normal.

- When installing or recreating volume groups or logical volumes from this backup, you cannot change the following attributes:
 - Any file system attributes
 - Logical volume name
 - Logical volume size
 - The volume group in which you want to create a logical volume

Backup file ID

Default=date/time (MMDDhhmm). Uniquely identifies the backup. You can change this field to any value but it cannot contain single (') or double (") quotes. This field is active only when you back up to a disk image file.

Dynamically Created Backup File ID

This option lets you generate a dynamic backup file ID. It uses the same current date and time values at the time of command execution as the ID. If the value of the Backup File ID field set to yes, it will overwrite the Backup File ID field.

Report output type

Default=progress indicator. Keep the default value if you want to display a progress indicator during the backup process, which indicates the approximate total backup time and amount completed. Press Tab to select "file list" if you want to display a list of files as they are being backed up, or Tab once more to show "only errors" that occur during the backup.

Platform/kernel type for tape boot image

Default=current platform/kernel type. This field is displayed only when you use a tape drive or virtual device. The field does not display a value if the current platform does not support tape boot or tape boot support is not installed. Change this field only if you are creating a backup that you want to install (clone) onto another platform type or to a machine running a different kernel. Press F4 to list the platforms/kernels that have tape boot support installed on the system and select from the list.

The following platform/kernel types are currently supported:

chrp	Common Hardware Reference Platform
chrp/MP	Multiprocessor Common Hardware Reference Platform
rs6k	RISC System/6000 (uniprocessor)
rs6k/MP	Multiprocessor RISC System/6000
rspc	PCI-based (PC) RISC System/6000 (uniprocessor)
rspc/MP	Multiprocessor PCI-based (PC) RISC System/6000

The first part of the selection is the platform type. The second part (/MP) indicates the kernel type. If the kernel type portion is omitted, a uniprocessor (single processor) kernel is assumed.

Network install support to include

Default=(Blank/None). If, after starting a system from this backup tape, you want the ability to perform a network installation (rather than installing from this backup), press F4 to display a list of supported network types and select one from the list. You must select the network type of the adapter that you want to use to install the system from the network.

Include non-JFS logical volumes?

Default=yes. To exclude all non-journaled file systems (raw logical volumes) from the backup, press Tab to change the value to "no". If you select "no" to this option, all raw logical volume data is excluded from the backup, but the logical volumes can be recreated using the LVM information on the backup. If you select "yes", all raw logical volumes are included on the backup *unless* you specifically excluded them in the *exclude list*.

Rewind tape before starting backup?

Default=yes. Press Enter to rewind the tape before the backup begins. If you are placing multiple backup images onto a single tape, then select "no" to place this backup on the tape at the current location. This option is displayed only when you back up to a tape device. For a system backup, tape boot information is placed on the tape at the beginning of the first backup. This information is not placed on the tape for subsequent backups.

Note: If this is the first backup to this tape, or if you have restarted the system, reinserted the tape, or changed the tape drive block size, you should select to rewind the tape. Only if you completed another backup and have not performed any of these functions will the tape be positioned correctly at the end of the previous backup image.

Forward to End of Tape Before Starting Backup

This option lets you fast forward to the end of the last SysBack backup on the tape for all backup types. Use this option when stacking multiple backups on the same tape that has been rewound or ejected. This options should also be used when the system has been restarted or the block size of the tape driver has been changed from the last backup. This eliminates having to manually position the tape before stacking a backup image.

Compress data before writing to media?

Default="no" for tapes and "yes" for disk image backups. Press Tab to change the option. "yes" indicates that the data will be compressed before it is written to the backup media.

Compressing the data usually increases backup performance and uses between 25 and 40% less space on the media. For best performance, do not select this option if the backup device provides its own hardware data compression. Compressing data with the software uses considerably more CPU cycles to process the data.

User description

Default=(Blank/None). Enter up to 60 characters of descriptive information to add to the volume label on the backup. Do not use single (') or double (") quotation marks in the description.

Host read permission

Default=all hosts. By default, all hosts with access to the system on which this file is written have permission to read, or restore from this image. Press Tab to limit read permission to the original host or the server on which the file is written. This option is active only when you back up to a disk image file.

User read permission

Default=all users. By default, any user on a host with access to the system and directory on which this file is written has permission to read, or restore from, this image. Press Tab to limit the read permission to only the original user, the root user on the original host, or the server to which the file is written. This option is active only when you back up to a disk image file.

Buffer size (In Kbytes)

Default=64. Changing this value either increases or decreases the amount of data that is written to the output device in a single I/O operation. Some devices with small buffers might require you to reduce this value, while other devices with very large buffers can benefit from increased performance by increasing this value. If you are unsure, use the default value. This value must be a multiple of the tape block size.

Preserve physical partition mapping?

Default=no. Selecting "yes" to this option ensures that all logical volumes will be recreated from this backup using the same physical partitions that are currently allocated to them. Unless the logical volumes were originally created using physical partition maps, it is generally recommended that they not be recreated using the same partitions, because this preserves fragmentation that develops over time as logical volumes and file systems expand.

When you recreate a volume group or logical volume or perform a system installation, you can choose whether or not to use the prior partition map. If the original physical volumes do not exist or are not large enough to contain the same partitions, the logical volumes will be recreated without using the maps.

Device name for remote volume prompt

Default=(Blank/None). Enter a TTY, LFT or PTS device name to send the volume prompt to a specified device rather than to the current SMIT screen. If you are backing up to a remote host, the device name you specify is attached to the remote host. This field is displayed only when the backup device is a tape drive or virtual device.

Examples of device names are `/dev/tty0`, `/dev/lft0` and `/dev/pts/5`. You can determine the terminal device name by typing `tty` at the command line on that device.

Overwrite existing backup with same ID?

Default=no. If the Backup File ID field contains a value already

used for an existing system backup, change this field to “yes” by pressing Tab. Doing so indicates that you want to overwrite the previous backup with this backup. After you begin this backup, the prior disk image files are removed and cannot be recovered. This field is displayed only when you back up to a disk image file.

CD/DVD Media Size

Specify the total size of the CD / DVD media in megabytes. If a backup image exceeds this length, it will be split. Each image that is split will have a number appended to the Backup file image name. For example: If the backup file SB.sysback1.hd2 needs to be split another file called SB.sysback1.hd2.2 would then be created automatically. Each time another split occurs that number is appended. In the case of double sided media, you should only specify the size of one side of the media, not the total aggregate size. This is a required option when the backup device is a directory and this backup image will later be burned to CD / DVD. The option does not apply to backups to tape or TSM virtual devices. Using this option also requires the use of the **Media Available Space** option.

Media Available Space

Specify the total size left on current CD DVD media in megabytes. This value is used only when creating the first CD/DVD image on CD1. It is the total size left after creating the boot images, adding the device filesets and populating the CD file system with all of the system files required on a system boot. If you are not sure what the exact value is for your environment, you may use the **CD/DVD Media Size** size less 125MB as this would accommodate the majority of environments for the size of all the items listed above. For example, if you had:

- 50 MB for device support filesets if added
- 25 MB for MCA boot image
- 25 MB for RSPC boot image
- 25 MB for CHRP boot image

The total is 125MB. If you wanted to create a boot CD to support RSPC and CHRP systems, and include needed device support, you would need to subtract 100MB from the **CD/DVD Media Size** size and use that value here. If no value is specified, the default value is 125. If a backup image exceeds this length it will be split. Each image that is split will have a number appended to the Backup file image name. For example: If the backup file SB.sysback1.hd2 needs to be split, another file called SB.sysback1.hd2.2 would then be created automatically. Each time another split occurs, that number is appended at the end and would then be increased by one. This is a required option when the backup device is a directory and this backup image will later be burned to CD / DVD. The option does not apply to backups to tape or TSM virtual devices. Using this option also requires the use of the **CD/DVD Media Size** option.

Format backup image on a 2gb limit?

This is a required option when the backup device is a directory and this backup will later be burned to CD / DVD. The option

does not apply to backups to tape or TSM virtual devices. Using this option also requires the use of the **Media Available Space** and **CD/DVD Media Size** options.

Non-rootvg Volume Groups to include

Default displays the volume groups previously selected, if any. You can add or delete volume groups from this list to include or exclude them from the backup. You can also press F4 to list the available volume groups and select from the list using F7.

5. After verifying all selections made above, press Enter to begin the backup.

If you selected to back up to tape, the tape block size is automatically changed to 512-byte blocks for writing the boot and installation images on the tape. This is necessary for the installation process to properly read the tape. After the boot and installation images are written to the tape, the block size is changed back to the original value and the remainder of the backup is written.

This process calculates and records certain information about your system configuration for later use by the installation process. The boot images are then placed on the tape, followed by each file system or logical volume in the selected volume groups.

Pre-Backup Script: If you created a custom script to run before the system backup, it runs first. This script might mail a message to users, remove temporary files, stop applications, or other similar functions. Refer to Appendix D, “Creating Scripts for Customizing the System Backup and Install Process”, on page D-1 for information on creating pre-backup scripts.

Post-Backup Script: If you created a custom script to run after the completion of the system backup, it runs after the backup is complete and before the tape is rewound and verified. This script might mail a message to users or re-enable applications that were disabled prior to the backup starting. Refer to Appendix D, “Creating Scripts for Customizing the System Backup and Install Process”, on page D-1 for information on creating post-backup scripts.

Backing up Volume Groups

If your system is organized so that the physical volumes, or hard disks, are placed into separate volume groups, then you probably want to back up these volume groups independently, for the following reasons.

First, data in different volume groups might require backups to be performed at different frequencies. For instance, critical data changed daily should be backed up at least once daily. Application programs or history files might not change on a daily basis and might be only backed up on a weekly or monthly basis.

Secondly, the most common hardware failure in any computer system is a hard disk failure. If a single disk fails within a volume group, you want to replace the disk and restore only the data in that one volume group. Separately backing up each volume group enables you to restore only a single volume group without touching the rest of the data on the system.

You can use the **Backup Volume Groups** option to back up one or more volume groups. All file systems and logical volumes in the selected volume groups are included on the backup unless they are specified in the exclude list.

Note: Do not use this option to back up the files in the rootvg volume group. To create a backup of the rootvg volume group or all volume groups, which can be used to reinstall the system, use the **Backup the System (Installation Image)** option. If you use the **Backup Volume Groups** option to backup the rootvg volume group, you can restore individual files from the backup but cannot reinstall the system.

Files, directories, or logical volumes contained in the *exclude list* are not included in the backup. If a file system mount point is contained in the exclude list, the entire file system is ignored. However, the information pertaining to all file systems and logical volumes is recorded to enable the recreation of the file systems or logical volumes as requested.

Before performing a volume group backup, log in to the system as a root user. This ensures that you have the appropriate permissions to read all of the files in the volume groups.

To back up one or more volume groups:

1. From the Backup Options menu, select **Backup Volume Groups**.

Note: From a command line, type `smit sb_mkvback`.

2. Select the volume group or groups to include in the backup from the list displayed. To select a single group, highlight the group and press Enter. To select multiple groups, highlight each group and press F7. Then, press Enter to continue.
3. On the Device Selector screen, highlight the device you want to use and press Enter.
4. One of the following screens is displayed. These screens show the default options and values available when you back up to either a local tape drive or a disk image file.

Backup a Volume Group

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

	[Entry Fields]	
Backup Data Hostname	hambone.austin.ibm.com	
Device name	/dev/rmt0	
Report output type	progress indicator	+
Rewind tape before starting backup?	yes	+
Forward to End of Tape Before Starting Backup	no	+
Compress data before writing to media?	no	+
Incremental backup level (0=full)	<input type="checkbox"/>	#
Include non-JFS logical volumes?	yes	+
User description	<input type="checkbox"/>	
Buffer size (in Kbytes)	[64]	+#
Preserve physical partition mapping?	no	+
Device name for remote volume prompt	<input type="checkbox"/>	
Exclude List File Name	<input type="checkbox"/>	+/
Hostname to Backup	<input type="checkbox"/>	
* Volume Group name(s)	[datavg]	+
[MORE]		

F1=Help
F5=Reset
F9=Shell

F2=Refresh
F6=Command
F10=Exit

F3=Cancel
F7=Edit
Enter=Do

F4=List
F8=Image

Figure 4-4. Default Options and Values Available When Backing Up to a Local Tape Drive

Backup a Volume Group

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

	[Entry Fields]	
Backup Data Hostname	hambone.austin.ibm.com	
Images directory	/sysback.images/fatrat>	
* Backup file ID	[03071030]	
Dynamically Created Backup File ID	no	+
Report output type	progress indicator	+
Compress data before writing to media?	yes	+
Incremental backup level (0=full)	<input type="checkbox"/>	#
Include non-JFS logical volumes?	yes	+
User description	<input type="checkbox"/>	
Host read permission	all hosts	+
User read permission	all users	+
Buffer size (in Kbytes)	[64]	+#
Preserve physical partition mapping?	no	+
Overwrite existing backup with same ID?	no	+
* Volume Group name(s)	[datavg]	+
[MORE]		

F1=Help
F5=Reset
F9=Shell

F2=Refresh
F6=Command
F10=Exit

F3=Cancel
F7=Edit
Enter=Do

F4=List
F8=Image

Figure 4-5. Default Options and Values Available When Backing Up to Disk Image File

The fields have the following definitions:

Backup Data Hostname:

The hostname of the data destination system on which the selected backup device or file exists. You may edit this field as

necessary to specify a the hostname of a remote system not listed in the device selector dialog screen. This is useful when initiating a Pull Backup.

Device name The device, if a tape drive or virtual device was selected. You may edit this field as necessary to specify a device on a remote system not listed in the device selector dialog screen. This is useful when initiating a Pull Backup.

Images directory
The directory name, if previously selected. You cannot change this field from this screen.

Backup file ID
Default=date/time (MMDDhhmm). Uniquely identifies the backup. You can change this field to any value but it cannot contain single (') or double (") quotes. This field is active only when you back up to a disk image file.

Dynamically Created Backup File ID
Generates a dynamic backup file ID. This option uses the same current date and time values at the time of command execution as the ID. If a dynamic backup file ID already exists and this option is set to "yes", the existing ID is overwritten.

Report output type
Default=progress indicator. Keep the default value if you want to display a progress indicator during the backup process, which indicates the approximate total backup time and amount completed. Press Tab to select "file list" if you want to display a list of files as they are being backed up, or Tab once more to show "only errors" that occur during the backup.

Compress data before writing to media?
Default="no" for tapes and "yes" for disk image backups. Press Tab to change the option. "yes" indicates that the data will be compressed before it is written to the backup media. Compressing the data usually increases backup performance and uses between 25 and 40% less space on the media. For best performance, do not select this option if the backup device provides its own hardware data compression. Compressing with software data uses considerably more CPU cycles to process the data.

Incremental backup level (0=full)
Default=(Blank/None). To perform an incremental backup of the volume group, enter an incremental level. Level 0 indicates a backup of all files and logical volumes. Leaving this field blank also backs up all files and logical volumes but the previous level 0 incremental backup information, if any, is not overwritten. Refer to "Understanding Incremental Backups" on page 4-1 for additional details.

Include non-JFS logical volumes?
Default=yes. To exclude all non-journaled file systems (raw logical volumes) from the backup, press Tab to change the value to "no". If you select "no" to this option, all raw logical volume data is excluded from the backup, but the logical volumes can be recreated using the LVM information on the

backup. If you select “yes”, all raw logical volumes are included on the backup *unless* you specifically excluded them in the *exclude list*.

User description

Default=(Blank/None). Enter up to 60 characters of descriptive information to add to the volume label on the backup. Do not use single (') or double (") quotation marks in the description.

Host read permission

Default=all hosts. By default, all hosts with access to the system on which this file is written have permission to read, or restore from, this image. Press Tab to limit read permission to the original host or the server on which the file is written. This option is displayed only when you back up to a disk image file.

User read permission

Default=all users. By default, any user on a host with access to the system and directory on which this file is written has permission to read, or restore from, this image. Press Tab to limit the read permission to only the original user, the root user on the original host, or the server to which the file is written. This option is displayed only when you back up to a disk image file.

Rewind tape before starting backup?

Default=yes. Press Enter to rewind the tape before the backup begins. If you are placing multiple backup images onto a single tape, then select “no” to place this backup on the tape at the current location. This option is displayed only when you back up to a tape device. For a system backup, tape boot information is placed on the tape at the beginning of the first backup. This information is not placed on the tape for subsequent backups.

Note: If this is the first backup to this tape, or if you have restarted the system, reinserted the tape, or changed the tape drive block size, you should select to rewind the tape. Only if you completed another backup and have not performed any of these functions will the tape be positioned correctly at the end of the previous backup image.

Forward to End of Tape Before Starting Backup

Forwards to the end of the last SysBack backup on the tape for all backup types. Use this option when stacking multiple backups on a tape that has been rewound or ejected. Also use this option options when the system has been restarted or when the block size of the tape drive has been changed from the last backup.

Buffer size (In Kbytes)

Default=64. Changing this value either increases or decreases the amount of data that is written to the output device in a single I/O operation. Some devices with small buffers might require you to reduce this value, while other devices with very large buffers can benefit from increased performance by increasing this value. If you are unsure, use the default value. This value must be a multiple of the tape block size.

Preserve physical partition mapping?

Default=no. Selecting “yes” to this option ensures that all logical volumes will be recreated from this backup using the same physical partitions that are currently allocated to them. Unless the logical volumes were originally created using physical partition maps, it is generally recommended that they not be recreated using the same partitions, because this preserves fragmentation that develops over time as logical volumes and file systems expand.

When you recreate a volume group or logical volume or perform a system installation, you can choose whether or not to use the prior partition map. If the original physical volumes do not exist or are not large enough to contain the same partitions, the logical volumes will be recreated without using the maps.

Device name for remote volume prompt

Default=(Blank/None). Enter a TTY, LFT or PTS device name to send the volume prompt to a specified device rather than to the current SMIT screen. If you are backing up to a remote host, the device name you specify is attached to the remote host. This field is displayed only when the backup device is a tape drive or virtual device.

Examples of device names are `/dev/tty0`, `/dev/lft0` and `/dev/pts/5`. You can determine the terminal device name by typing `tty` at the command line on that device.

Overwrite existing backup with same ID?

Default=no. If the Backup File ID field contains a value already used for an existing system backup, change this field to “yes” by pressing Tab. Doing so indicates that you want to overwrite the previous backup with this backup. After you begin this backup, the prior disk image files are removed and cannot be recovered. This field is displayed only when you back up to a disk image file.

Hostname to Backup

The hostname of the backup system, the machine that will send its data to the data destination server.

Exclude List File Name

Specify the full qualified path and file name of a SysBack exclude list. If this field is left blank, the backup process will process the contents of `/usr/lpp/sysback/exclude_list` automatically.

Volume Group name(s)

The volume groups selected on the first selection screen, each separated by spaces. You can change the list by adding or removing volume group names, or you can press F4 to list the volume groups on the system and F7 to select each volume group from the list. All volume groups indicated in this field are included in this backup.

5. After confirming the above entries, make sure the backup media is properly inserted in the drive and press Enter to begin the backup.

Note: If you are backing up to a tape drive, the tape will NOT be rewound upon completion of the backup. This enables you to perform additional backups (also without rewinding), thereby “stacking” the backups onto a single tape.

Backing up File systems

A file system backup can only be performed for mounted (active) file systems. Various file systems are often backed up at different intervals from each other or from the volume group or system backup, because the data in different file systems is changed at different intervals.

Because file systems are contained in the system and volume group backups, you do not need to back them up separately, unless you want to back up this data independently or more frequently.

All files and directories in the file systems are included in the backup unless you specify them in the exclude list. If the mount point of a file system to be backed up is also in the exclude list, the backup of the file system continues, but no files in the file system are included.

Before performing a file system backup, log in to the system as a root user. This ensures that you have the appropriate permissions to read all of the files in the file systems.

To back up one or more file systems:

1. From the Backup Options menu, select **Backup file systems**.

Note: From a command line, type `smit sb_mkfsback`.

2. Select a file system from the list of file system mount points. To select a single file system, highlight a directory and press Enter. To select multiple file systems, highlight each directory and press F7. When you’ve made all your selections, press Enter.
3. On the Device Selector screen, highlight the device you want to use and press Enter.
4. One of the following screens is displayed. These screens show the default options and values available when you back up to either a local tape drive or a disk image file.

Backup a Filesystem

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

	[Entry Fields]
Backup Data Hostname	hambone.austin.ibm.com
Device name	/dev/rmt0
Report output type	progress indicator +
Forward to End of Tape Before Starting Backup	no +
Rewind tape before starting backup?	yes +
Compress data before writing to media?	no +
Incremental backup level (0=full)	[] #
User description	[]
Buffer size (in Kbytes)	[64] + #
Preserve physical partition mapping?	no +
Device name for remote volume prompt	[]
* Filesystem(s) (directory names)	[/tivoli] + /
[MORE]	

F1=Help
F5=Reset
F9=Shell

F2=Refresh
F6=Command
F10=Exit

F3=Cancel
F7=Edit
Enter=Do

F4=List
F8=Image

Figure 4-6. Default Options and Values Available When Backing Up to a Local Tape Drive

Backup a Filesystem

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

	[Entry Fields]
Backup Data Hostname	hambone.austin.ibm.com
Images directory	/sysback.images/fatrat>
* Backup file ID	[03071032]
Dynamically Created Backup File ID	no +
Report output type	progress indicator +
Compress data before writing to media?	yes +
Incremental backup level (0=full)	[] #
User description	[]
Host read permission	all hosts +
User read permission	all users +
Buffer size (in Kbytes)	[64] + #
Preserve physical partition mapping?	no +
Overwrite existing backup with same ID?	no +
* Filesystem(s) (directory names)	[/tivoli] + /
[MORE]	

F1=Help
F5=Reset
F9=Shell

F2=Refresh
F6=Command
F10=Exit

F3=Cancel
F7=Edit
Enter=Do

F4=List
F8=Image

Figure 4-7. Default Options and Values Available When Backing Up to Disk Image File

The fields have the following definitions:

Backup Data Hostname

This field contains the hostname of the backup server on which the selected backup device or file exists. You may edit this field as necessary to specify a the hostname of a remote system not listed in the device selector dialog screen. This is useful when initiating a Pull Backup.

Device name The device, if a tape drive or virtual device was selected. You

may edit this field as necessary to specify a device on a remote system not listed in the device selector dialog screen. This is useful when initiating a Pull Backup.

Images directory

The directory name, if previously selected. You cannot change this field from this screen.

Create a Power Backup?

Default=no. Use Tab to change this field to “yes” if you want this backup to be a “Power” backup. A Power backup backs up all file systems as “raw” logical volumes, which usually provides much better backup and restore performance, but imposes the following limitations:

- You can restore only raw logical volumes from this backup. Therefore, when choosing to restore data from the backup, you will be allowed to restore only an entire logical volume and only if it is inactive. Because of this, you cannot restore any individual files or directories, only entire file systems; and no file systems, such as /, /usr and /var can be restored since they are always active.
- Because all file systems are backed up as raw logical volumes, the entire logical volume is backed up even if only one-fourth of the file system is used. If this were the case with all file systems, the backup and installation would likely take longer than normal.
- When installing or recreating volume groups or logical volumes from this backup, you cannot change the following attributes:
 - Any file system attributes
 - Logical volume name
 - Logical volume size
 - The volume group in which you want to create a logical volume

Backup file ID

Default=date/time (MMDDhhmm). Uniquely identifies the backup. You can change this field to any value but it cannot contain single (') or double (") quotes. This field is active only when you back up to a disk image file.

Dynamically Created Backup File ID

Generates a dynamic backup file ID. This option uses the same current date and time values at the time of command execution as the ID. If a dynamic backup file ID already exists and this option is set to “yes”, the existing ID is overwritten.

Report output type

Default=progress indicator. Keep the default value if you want to display a progress indicator during the backup process, which indicates the approximate total backup time and amount completed. Press Tab to select “file list” if you want to display a list of files as they are being backed up, or Tab once more to show “only errors” that occur during the backup.

Compress data before writing to media?

Default=“no” for tapes and “yes” for disk image backups. Press

Tab to change the option. “yes” indicates that the data will be compressed before it is written to the backup media. Compressing the data usually increases backup performance and uses between 25 and 40% less space on the media. For best performance, do not select this option if the backup device provides its own hardware data compression. Compressing data with software uses considerably more CPU cycles to process the data.

Incremental backup level (0=full)

Default=(Blank/None). To perform an incremental backup of the volume group, enter an incremental level. Level 0 indicates a backup of all files and logical volumes. Leaving this field blank also backs up all files and logical volumes but the previous level 0 incremental backup information, if any, is not overwritten. Refer to “Understanding Incremental Backups” on page 4-1 for additional details.

User description

Default=(Blank/None). Enter up to 60 characters of descriptive information to add to the volume label on the backup. Do not use single (') or double (") quotation marks in the description.

Host read permission

Default=all hosts. By default, all hosts with access to the system on which this file is written have permission to read, or restore from, this image. Press Tab to limit read permission to the original host or the server on which the file is written. This option is displayed only when you back up to a disk image file.

User read permission

Default=all users. By default, any user on a host with access to the system and directory on which this file is written has permission to read, or restore from, this image. Press Tab to limit the read permission to only the original user, the root user on the original host, or the server to which the file is written. This option is displayed only when you back up to a disk image file.

Rewind tape before starting backup?

Default=yes. Press Enter to rewind the tape before the backup begins. If you are placing multiple backup images onto a single tape, then select “no” to place this backup on the tape at the current location. This option is displayed only when you back up to a tape device. For a system backup, tape boot information is placed on the tape at the beginning of the first backup. This information is not placed on the tape for subsequent backups.

Note: If this is the first backup to this tape, or if you have restarted the system, reinserted the tape, or changed the tape drive block size, you should select to rewind the tape. Only if you completed another backup and have not performed any of these functions will the tape be positioned correctly at the end of the previous backup image.

Forward to End of Tape Before Starting Backup

Forwards to the end of the last SysBack backup on the tape for all backup types. Use this option when stacking multiple

backups on a tape that has been rewound or ejected. Also use this option when the system has been restarted or when the block size of the tape driver has been changed from the last backup.

Buffer size (In Kbytes)

Default=64. Changing this value either increases or decreases the amount of data that is written to the output device in a single I/O operation. Some devices with small buffers might require you to reduce this value, while other devices with very large buffers can benefit from increased performance by increasing this value. If you are unsure, use the default value. This value must be a multiple of the tape block size.

Preserve physical partition mapping?

Default=no. Selecting “yes” to this option ensures that all logical volumes will be recreated from this backup using the same physical partitions that are currently allocated to them. Unless the logical volumes were originally created using physical partition maps, it is generally recommended that they not be recreated using the same partitions, because this preserves fragmentation that develops over time as logical volumes and file systems expand.

When you recreate a volume group or logical volume or perform a system installation, you can choose whether or not to use the prior partition map. If the original physical volumes do not exist or are not large enough to contain the same partitions, the logical volumes will be recreated without using the maps.

Device name for remote volume prompt

Default=(Blank/None). Enter a TTY, LFT or PTS device name to send the volume prompt to a specified device rather than to the current SMIT screen. If you are backing up to a remote host, the device name you specify is attached to the remote host. This field is displayed only when the backup device is a tape drive or virtual device.

Examples of device names are `/dev/tty0`, `/dev/lft0` and `/dev/pts/5`. You can determine the terminal device name by typing `tty` at the command line on that device.

Overwrite existing backup with same ID?

Default=no. If the Backup File ID field contains a value already used for an existing system backup, change this field to “yes” by pressing Tab. Doing so indicates that you want to overwrite the previous backup with this backup. After you begin this backup, the prior disk image files are removed and cannot be recovered. This field is displayed only when you back up to a disk image file.

Hostname to Backup

The hostname of the backup system, the machine that will send its data to the data destination server.

Exclude List File Name

Specify the full qualified path and file name of a SysBack exclude list. If this field is left blank, the backup process will process the contents of `/usr/lpp/sysback/.exclude_list` automatically.

File system(s) (directory names)

The file system mount points (directories) selected on the first selection screen, each separated by spaces. You can change the list by adding or removing file systems, or you can press F4 to list the mounted file systems on the system and use F7 to select one or more from the list. All file systems in this field, unless included in the exclude list, are included in this backup.

Directory names should be specified relative to the root (/) directory.

5. After confirming the above entries, make sure the backup media is properly inserted in the drive and press Enter to begin the backup.

Note: If you are backing up to a tape drive, the tape will NOT be rewound upon completion of the backup. This enables additional backups to be performed (also without rewinding), thereby “stacking” the backups onto a single tape.

Backing up Logical Volumes

This option is typically used to back up logical volumes that contain non-file system data, such as data written by various database products or custom applications.

Logical volumes are contained in the system and volume group backups, so you do not need to back them up separately, unless you want to back up this data independently or more frequently.

You can use this option to backup a file system logical volume only if the file system is unmounted before the backup is performed. For non-file system logical volumes, the backup can be performed even if the logical volume is active, but it is recommended that data not be changed in the logical volume during the backup to ensure the consistency of relational data during the backup.

Since logical volume names must be explicitly selected using this option, they are backed up even if they are in the exclude list.

To backup one or more logical volumes:

1. From the Backup Options menu, select **Backup Logical Volumes**.

Note: From a command line, type `smit sb_mklvback`.

2. Select a logical volume from the list of non-file system logical volumes and logical volumes with unmounted file system. To select a single logical volume, highlight the name and press Enter. To select multiple logical volumes, highlight each volume group and press F7. When you’ve made all your selections, press Enter.
3. On the Device Selector screen, highlight the device you want to use and press Enter.
4. One of the following screens is displayed. These screens show the default options and values available when you back up to either a local tape drive or a disk image file.

Backup a Logical Volume			
Type or select values in entry fields. Press Enter AFTER making all desired changes.			
	[Entry Fields]		
Backup Data Hostname	hambone.austin.ibm.com		
Device name	/dev/rmt0		
Show progress indicator?	yes	+	
Rewind tape before starting backup?	yes	+	
Forward to End of Tape Before Starting Backup	no	+	
Compress data before writing to media?	no	+	
User description	[]		
Buffer size (in Kbytes)	[64]	+#	
Preserve physical partition mapping?	no	+	
Device name for remote volume prompt	[]		
* Logical Volume name(s)	[1v00]	+	
[MORE]			
F1=Help	F2=Refresh	F3=Cancel	F4=List
F5=Reset	F6=Command	F7=Edit	F8=Image
F9=Shell	F10=Exit	Enter=Do	

Figure 4-8. Default Options and Values Available When Backing Up to Tape

Backup a Logical Volume			
Type or select values in entry fields. Press Enter AFTER making all desired changes.			
	[Entry Fields]		
Backup Data Hostname	hambone.austin.ibm.com		
Images directory	/sysback.images/fatrat>		
* Backup file ID	[03071034]		
Dynamically Created Backup File ID	no	+	
Show progress indicator?	yes	+	
Compress data before writing to media?	yes	+	
User description	[]		
Host read permission	all hosts	+	
User read permission	all users	+	
Buffer size (in Kbytes)	[64]	+#	
Preserve physical partition mapping?	no	+	
Overwrite existing backup with same ID?	no	+	
* Logical Volume name(s)	[1v00]	+	
[MORE]			
F1=Help	F2=Refresh	F3=Cancel	F4=List
F5=Reset	F6=Command	F7=Edit	F8=Image
F9=Shell	F10=Exit	Enter=Do	

Figure 4-9. Default Options and Values Available When Backing Up to Disk Image File

The fields have the following definitions:

Backup Data Hostname

The hostname of the data destination system on which the selected backup device or file exists. You may edit this field as necessary to specify a the hostname of a remote system not listed in the device selector dialog screen. This is useful when initiating a Pull Backup.

Device name The device, if a tape drive or virtual device was selected. You

may edit this field as necessary to specify a device on a remote system not listed in the device selector dialog screen. This is useful when initiating a Pull Backup.

Images directory

The directory name, if previously selected. You cannot change this field from this screen.

Backup file ID

Default=date/time (MMDDhhmm). Uniquely identifies the backup. You can change this field to any value but it cannot contain single (') or double (") quotes. This field is active only when you back up to a disk image file.

Dynamically Created Backup File ID

Generates a dynamic backup file ID. This option uses the same current date and time values at the time of command execution as the ID. If a dynamic backup file ID already exists and this option is set to "yes", the existing ID is overwritten.

Show progress indicator?

Default="yes". Press Tab to change the value to "no" if you do not want the progress indicator shown on the screen during the backup.

Compress data before writing to media?

Default="no" for tapes and "yes" for disk image backups. Press Tab to change the option. "yes" indicates that the data will be compressed before it is written to the backup media.

Compressing the data usually increases backup performance and uses between 25 and 40% less space on the media. For best performance, do not select this option if the backup device provides its own hardware data compression. Compressing data with software uses considerably more CPU cycles to process the data.

User description

Default=(Blank/None). Enter up to 60 characters of descriptive information to add to the volume label on the backup. Do not use single (') or double (") quotation marks in the description.

Host read permission

Default=all hosts. By default, all hosts with access to the system on which this file is written have permission to read, or restore from, this image. Press Tab to limit read permission to the original host or the server on which the file is written. This option is displayed only when you back up to a disk image file.

User read permission

Default=all users. By default, any user on a host with access to the system and directory on which this file is written has permission to read, or restore from, this image. Press Tab to limit the read permission to only the original user, the root user on the original host, or the server to which the file is written. This option is displayed only when you back up to a disk image file.

Rewind tape before starting backup?

Default=yes. Press Enter to rewind the tape before the backup begins. If you are placing multiple backup images onto a single

tape, then select “no” to place this backup on the tape at the current location. This option is displayed only when you back up to a tape device. For a system backup, tape boot information is placed on the tape at the beginning of the first backup. This information is not placed on the tape for subsequent backups.

Note: If this is the first backup to this tape, or if you have restarted the system, reinserted the tape, or changed the tape drive block size, you should select to rewind the tape. Only if you completed another backup and have not performed any of these functions will the tape be positioned correctly at the end of the previous backup image.

Forward to End of Tape Before Starting Backup

Forwards to the end of the last SysBack backup on the tape for all backup types. Use this option when stacking multiple backups on a tape that has been rewound or ejected. Also use this option when the system has been restarted or when the block size of the tape driver has been changed from the last backup.

Buffer size (In Kbytes)

Default=64. Changing this value either increases or decreases the amount of data that is written to the output device in a single I/O operation. Some devices with small buffers might require you to reduce this value, while other devices with very large buffers can benefit from increased performance by increasing this value. If you are unsure, use the default value. This value must be a multiple of the tape block size.

Preserve physical partition mapping?

Default=no. Selecting “yes” to this option ensures that all logical volumes will be recreated from this backup using the same physical partitions that are currently allocated to them. Unless the logical volumes were originally created using physical partition maps, it is generally recommended that they not be recreated using the same partitions, because this preserves fragmentation that develops over time as logical volumes and file systems expand.

When you recreate a volume group or logical volume or perform a system installation, you can choose whether or not to use the prior partition map. If the original physical volumes do not exist or are not large enough to contain the same partitions, the logical volumes will be recreated without using the maps.

Device name for remote volume prompt

Default=(Blank/None). Enter a TTY, LFT or PTS device name to send the volume prompt to a specified device rather than to the current SMIT screen. If you are backing up to a remote host, the device name you specify is attached to the remote host. This field is displayed only when the backup device is a tape drive or virtual device.

Examples of device names are `/dev/tty0`, `/dev/lft0` and `/dev/pts/5`. You can determine the terminal device name by typing `tty` at the command line on that device.

Overwrite existing backup with same ID?

Default=no. If the Backup File ID field contains a value already used for an existing system backup, change this field to “yes” by pressing Tab. Doing so indicates that you want to overwrite the previous backup with this backup. After you begin this backup, the prior disk image files are removed and cannot be recovered. This field is displayed only when you back up to a disk image file.

Hostname to Backup

The hostname of the backup system, the machine that will send its data to the data destination server.

Exclude List File Name

Specify the full qualified path and file name of a SysBack exclude list. If this field is left blank, the backup process will process the contents of `/usr/lpp/sysback/.exclude_list` automatically.

Logical Volume name(s)

The logical volume name or names selected on the first selection screen, each separated by spaces. You can change the list by adding or removing logical volume names, or press F4 to list the valid logical volumes on the system and use F7 to select one or more from the list.

5. After confirming the above entries, make sure the backup media is properly inserted in the drive and press Enter to begin the backup.

Note: If you are backing up to a tape drive, the tape will NOT be rewound upon completion of the backup. This enables additional backups to be performed (also without rewinding), thereby “stacking” the backups onto a single tape.

During the backup, the Progress Indicator will be displayed, indicating the estimated backup time, and the amount completed.

Backing up Files or Directories

Use this option to back up a single file or directory or a group of files or directories. You can also back up only the files that have changed within a certain number of days. This enables the files or directories specified to be backed up incrementally from day to day. For instance, you might choose to back up all files in a directory each Friday evening. Then, for each following day, you can choose to back up only the files that have changed in the last day. Keep in mind the following when using this option:

- One day equals exactly 24 hours. Therefore, if you perform a backup of a file at 1:00 am on Tuesday, and the same file is not read until 3:00 am on Wednesday, it will not be backed up if it was changed at 2:00 am on Tuesday, 25 hours ago. If files are changed during the backup period, it is often best to add an extra day to the backup increment for safety.
- For each sequential backup of a directory in which only one day of data is backed up, it might be necessary to perform many restores of many backups to restore the entire directory from scratch. For instance, if the directory was backed up in its entirety on the first of the month, and only a single day of changes was backed up each following day, it will take a restore from 22 different tapes to restore the entire directory on the 22nd day of the month.

Unlike all other backup types, this type of backup contains no Logical Volume Manager (LVM) information. Therefore, you cannot use this backup, regardless of its contents, to recreate volume groups, logical volumes, or file systems. Using this backup option for backing up all files on the system (from the / directory) does *not* provide a backup that can be used to reinstall the system.

It is also important to note that some files and directories on the system, such as certain contents of the root (/) and /usr file systems, should never be restored from a backup, as this would adversely affect the active system configuration and can cause either system errors or a complete system failure. Use this option only to back up files and directories that contain non-system-related information, such as user data and application programs.

To back up files or directories:

1. From the Backup Options menu, select **Backup Files or Directories**.

Note: From a command line, type `smit sb_mkdirback`.

2. On the Device Selector screen, highlight the device you want to use and press Enter.
3. One of the following screens is displayed. These screens show the default options and values available when you back up to either a local tape drive or a disk image file.

Backup Files or Directories

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

	[Entry Fields]	
Backup Data Hostname	hambone.austin.ibm.com	
Device name	/dev/rmt0	
Report output type	progress indicator	+
Rewind tape before starting backup?	yes	+
Forward to End of Tape Before Starting Backup	no	+
Compress data before writing to media?	no	+
Backup only files changed within #days (0=all)	[0]	#
User description	[]	
Buffer size (in Kbytes)	[64]	+#
Device name for remote volume prompt	[]	
* File(s) or starting directory(s)	[/tivoli/TEC /home/gues> +	
[MORE]		

F1=Help
F2=Refresh
F3=Cancel
F4=List

F5=Reset
F6=Command
F7=Edit
F8=Image

F9=Shell
F10=Exit
Enter=Do

Figure 4-10. Default Options and Values Available When Backing Up to Tape

Backup Files or Directories

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

	[Entry Fields]
Backup Data Hostname	hambone.austin.ibm.com
Images directory	/sysback.images/fatrat>
* Backup file ID	[03071041]
Dynamically Created Backup File ID	no +
Report output type	progress indicator +
Compress data before writing to media?	yes +
Backup only files changed within #days (0=all)	[0] #
User description	[]
Host read permission	all hosts +
User read permission	all users +
Buffer size (in Kbytes)	[64] +#
Overwrite existing backup with same ID?	no +
* File(s) or starting directory(s)	[/tivo/TEC /home/gues> +
[MORE]	

F1=Help

F2=Refresh

F3=Cancel

F4=List

F5=Reset

F6=Command

F7=Edit

F8=Image

F9=Shell

F10=Exit

Enter=Do

Figure 4-11. Default Options and Values Available When Backing Up to Disk Image File

The fields have the following definitions:

Backup Data Hostname

The hostname of the data destination system on which the selected backup device or file exists. You may edit this field as necessary to specify a the hostname of a remote system not listed in the device selector dialog screen. This is useful when initiating a Pull Backup.

Device name The device, if a tape drive or virtual device was selected. You may edit this field as necessary to specify a device on a remote system not listed in the device selector dialog screen. This is useful when initiating a Pull Backup.

Images directory

The directory name, if previously selected. You cannot change this field from this screen.

Backup file ID

Default=date/time (MMDDhhmm). Uniquely identifies the backup. You can change this field to any value but it cannot contain single (') or double (") quotes. This field is active only when you back up to a disk image file.

Dynamically Created Backup File ID

Generates a dynamic backup file ID. This option uses the same current date and time values at the time of command execution as the ID. If a dynamic backup file ID already exists and this option is set to "yes", the existing ID is overwritten.

Report output type

Default=progress indicator. Keep the default value if you want to display a progress indicator during the backup process, which indicates the approximate total backup time and amount completed. Press Tab to select "file list" if you want to display

a list of files as they are being backed up, or Tab once more to show “only errors” that occur during the backup.

Compress data before writing to media?

Default=“no” for tapes and “yes” for disk image backups. Press Tab to change the option. “yes” indicates that the data will be compressed before it is written to the backup media.

Compressing the data usually increases backup performance and uses between 25 and 40% less space on the media. For best performance, do not select this option if the backup device provides its own hardware data compression. Compressing data with software uses considerably more CPU cycles to process the data.

Backup only files changed since #days (0=all)

Default=0. To backup only the files that have changed within a certain number of days, enter the number of days here. If, for instance, your last file or directory backup was at this time yesterday, enter “1” to backup all files changed since that time. Note that a day is considered exactly 24 hours, so if your backup was earlier in the day yesterday than it was today, you should backup at least two days of changes.

User description

Default=(Blank/None). Enter up to 60 characters of descriptive information to add to the volume label on the backup. Do not use single (') or double (") quotation marks in the description.

Host read permission

Default=all hosts. By default, all hosts with access to the system on which this file is written have permission to read, or restore from, this image. Press Tab to limit read permission to the original host or the server on which the file is written. This option is displayed only when you back up to a disk image file.

User read permission

Default=all users. By default, any user on a host with access to the system and directory on which this file is written has permission to read, or restore from, this image. Press Tab to limit the read permission to only the original user, the root user on the original host, or the server to which the file is written. This option is displayed only when you back up to a disk image file.

Rewind tape before starting backup?

Default=yes. Press Enter to rewind the tape before the backup begins. If you are placing multiple backup images onto a single tape, then select “no” to place this backup on the tape at the current location. This option is displayed only when you back up to a tape device. For a system backup, tape boot information is placed on the tape at the beginning of the first backup. This information is not placed on the tape for subsequent backups.

Note: If this is the first backup to this tape, or if you have restarted the system, reinserted the tape, or changed the tape drive block size, you should select to rewind the tape. Only if you completed another backup and have

not performed any of these functions will the tape be positioned correctly at the end of the previous backup image.

Forward to End of Tape Before Starting Backup

Forwards to the end of the last SysBack backup on the tape for all backup types. Use this option when stacking multiple backups on a tape that has been rewound or ejected. Also use this option when the system has been restarted or when the block size of the tape driver has been changed from the last backup.

Buffer size (In Kbytes)

Default=64. Changing this value either increases or decreases the amount of data that is written to the output device in a single I/O operation. Some devices with small buffers might require you to reduce this value, while other devices with very large buffers can benefit from increased performance by increasing this value. If you are unsure, use the default value. This value must be a multiple of the tape block size.

Device name for remote volume prompt

Default=(Blank/None). Enter a TTY, LFT or PTS device name to send the volume prompt to a specified device rather than to the current SMIT screen. If you are backing up to a remote host, the device name you specify is attached to the remote host. This field is displayed only when the backup device is a tape drive or virtual device.

Examples of device names are `/dev/tty0`, `/dev/lft0` and `/dev/pts/5`. You can determine the terminal device name by typing `tty` at the command line on that device.

Overwrite existing backup with same ID?

Default=no. If the Backup File ID field contains a value already used for an existing system backup, change this field to "yes" by pressing Tab. Doing so indicates that you want to overwrite the previous backup with this backup. After you begin this backup, the prior disk image files are removed and cannot be recovered. This field is displayed only when you back up to a disk image file.

Hostname to Backup

The hostname of the backup system, the machine that will send its data to the data destination server.

Exclude List File Name

Specify the full qualified path and file name of a SysBack exclude list. If this field is left blank, the backup process will process the contents of `/usr/lpp/sysback/.exclude_list` automatically.

File(s) or starting directory(s)

Default=blank. Enter the starting directory where you want the backup to begin. You can enter multiple directory names if you want to back up all of these directories in a single backup. If you want to back up the entire contents of a file system, specify the mount point for that file system (for example, `/home`). Press F4 to obtain a list of all currently mounted local file systems and use F7 to select the starting directory from the list.

Directory names must be in one of the following formats:

- /directory/filename
- /directory
- ./filename
- ./directory/filename
- ./directory

All files will be backed up relative to the root (/) directory by automatically inserting a period (.) at the beginning of each filename, if it does not already exist. Otherwise, they are backed up relative to their file system mount point.

4. After confirming the above entries, make sure the backup media is properly inserted in the drive and press Enter to begin the backup.

Note: If you are backing up to a tape drive, the tape will *not* be rewound upon completion of the backup. This enables you to perform additional backups (also without rewinding), thereby “stacking” the backups onto a single tape.

Understanding Exclude List Processing on Backup Operations

Backup processes use the following rules when processing backup exclude lists:

- If `/usr/lpp/sysback/.exclude_list` exists, the contents are processed unless another path and file name are explicitly specified.
- If you have created an exclude list file in an alternate location, specifying its path and file name with the backup command will cause the backup to process the content of this file rather than the default. Even if the default `/usr/lpp/sysback/.exclude_list` file exists, it will be ignored for this iteration of the backup command.
- If you have an existing `/usr/lpp/sysback/.exclude_list` file, but would like to temporarily override it and exclude nothing, you could do this to avoid deleting the default exclude list:

```
root@lasher> touch /tmp/empty.excl  
sysback -f /dev/rmt0 -E /tmp/empty.excl
```

This would cause the backup command to process the contents of the empty file thereby excluding nothing.

Using SysBack with Fire Walls

SysBack currently opens the following ports by default on each side of a remote communication with another system:

- 1239
- 1023 for standard out
- 1022 for standard error

If ports 1023 and 1022 are not available, SysBack will decrement this number until it reaches a port not already. However, SysBack will not use a port number less than 512. At this time, there is no way to specify which ports SysBack will utilize and any SysBack remote services between systems separated by a firewall will require that the needed ports be opened. You must configure the firewall to open up the ports that the server and clients need. Because fire walls differ in how you open the ports, you must follow the instructions that accompanied the firewall software or hardware that you are using. If you need help with opening ports, please contact the supplier of your firewall.

Additionally, SysBack requires that reverse name resolution be the same on both sides of the firewall. Let us assume the following information:

System B = fruit, 9.19.125.19

If you were logged on to System A:

```
root:systemB> host apple
```

```
apple is 9.19.125.19
```

```
root:systemB> host 9.19.125.19
```

```
apple.dfw.ibm.com is 9.19.125.19
```

SysBack will think that apple and apple.dfw.ibm.com are two different hosts.

Backup Return Code Processing

When non-fatal errors are returned from the underlying backup command but still allow SysBack to continue, SysBack will exit with a return code one, or WARNING. The non-fatal errors could vary depending on the operating environment since the condition is usually predicated upon problems in AIX or from AIX commands. Therefore, during the backup you might see an error like: 0511-089 unable to open file xxxx out of memory

or other errors like:

```
File /somepath/somefile can not be found.
```

The later is often seen in environments that have ever changing temp file generation. The **/usr/sbin/backup** command continues on even when these conditions occur. These are considered soft errors because they don't impact the overall backup process.

When an error occurs that is unrecoverable, or threatens the completion of the overall backup process, SysBack will exit with a return code 2, or ERROR.

Backups that have no warnings or errors will exit with a return code one, or SUCCESS.

Therefore, the sysback, mkvgback, mkjfsback, mklvback, and mkdirback commands have three possible return codes:

- 0 Success
- 1 Warning, or soft failure
- 2 Error, or hard failure

At the end of the backup process, a message like the below will be displayed indicating the overall completion status of the backup process:

```
WARNING: Volume Group backup completed with non-fatal errors
```

It is always best to save stdout and stderr from all backup operations for review when running the backup in the background. This will allow you to easily review error conditions encountered should you receive a WARNING or ERROR message.

The easiest way to capture stdout and stderr is to append this string to the end of your backup command:

```
> /tmp/backup.log 2>&1
```

By adding this string instead, you will generate a unique log name based on the date and time with each backup:> /tmp/backup.log\$(date "+%m%d%H%M").log 2>&1

Unattended Backups Running in the Background

By default, if the backup command process is run through cron, nohup, or the “at” command and there is no controlling tty because the backup is running in the background, the backup process will terminate if the device (tape or virtual device) is:

- Not Ready
- Contains write protected media
- Contains no media at all

If you would like the process to wait indefinitely to be resolved, rather than to terminate, you should add the **-A** flag the: sysback, mkvgback, mklvback, mkjfsback, and mkdirback, commands.

If you also use the **-c /dev/termdev** flag to the backup command, a message will be displayed on the terminal when one of these conditions occur. If you do not use the **-c /dev/termdev** flag, and you have used the **-A** flag, SysBack will check to see if there is a controlling tty, and if there is not, it will use **-c /dev/console**.

When there is a controlling tty for the backup process, for example the backup is run in the foreground, the backup process will wait indefinitely if any of the aforementioned conditions are encountered. Once the condition is rectified, the process will continue.

This functionality only applies for the first tape in a backup (i.e.: when the back starts). If a backup spans to multiple tapes, and any subsequent tape meets any of the described criteria, then the backup process will wait until such time as this condition is corrected. Currently, the underlying commands will not display a message indicating that this condition has been encountered and the backup process may appear hung. This is a known limitation.

Chapter 5. Backups to CD or DVD

You may create a full system (installation image) backup to a CD or DVD. Other SysBack backup types may not be performed to CD or DVD. The `/usr/sbin/mksbcd` command, or its respective SMIT menu, is used to initiate a full system backups to CD or DVD.

Requirements

SysBack's CD and DVD backup feature has additional hardware and software requirements beyond the base product requirements. They are:

Software

- SysBack requires AIX (BOS) Version 4.3.0 or higher including AIX 5.1 and 5.2.
- See other optional AIX fileset requirements for use with certain SysBack features not related to CD or DVD support in Chapter 1, "Installation", on page 1-1.
- CD Support requires AIX 4.3.0 or higher.
- DVD Support requires AIX 4.3.3 or higher AND `bos.sysmgt.sysbr` must be 4.3.3.50 or higher. IY15536 will bring `bos.sysmgt.sysbr` to fix level 50.
- GNU software tools `mkisofs` and `readcd` which are included in the GNU `cdrecord` and `cdrtools` packages.

These tools may be obtained from the AIX for Linux Toolbox CD, download them from <http://www-1.ibm.com/servers/aix/products/aixos/linux/download.html> or download them from the internet website of your choice. IBM and Tivoli does not support these code packages.

Hardware

SysBack supports IBM's RS/6000 and @server pSeries servers. The following CD and DVD devices have been tested as of the date of this README. Other devices may also work with SysBack, but only these devices are officially supported. Use of other devices is at your own discretion as there is no guarantee of support for other devices. Your choice of device must not require vendor specific software for writing and reading. Although the AIX `/usr/sbin/mkcd` command supports the use of GNU Utilities, or a separately purchasable software from Jodian, SysBack ONLY supports the use of the GNU Utilities for reading and writing to the devices.

Essentially, if AIX supports the device with the use of GNU utilities, then SysBack will also support the use of the device with GNU Utilities. If AIX requires a certain level of the GNU Utilities, then SysBack will require that same level. At the time of this list, the following devices were all tested by either AIX or SysBack development and are formally supported. Below is the list of devices formally supported with SysBack (although other devices may also work):

- IBM 7210 Model 025 DVD-RAM Drive
- Other DVD - RAM Devices as supported by AIX
- Other DVD-R Devices as supported by AIX
- Other CD-R Devices as supported by AIX
- Other CD-RW supported by AIX

Note: SysBack supports any device supported that is support by AIX and does not require it's own proprietary drivers or software to operate. For a list of the devices explicitly supported / tested by AIX, at your operating system level, please see the file: `/usr/lpp/bos.sysmgmt/README.oem_writers`

We have specifically tested at the following levels:

- cdrecord 1.9.0.0
- cdrtools 1.10.23

We support the use of these levels of said GNU Tools as well as later levels provided through AIX maintenance level releases or the AIX for Linux Toolbox. GNU Tools newer than what is distributed via AIX software updates may not function consistently and support is not guaranteed. Once these GNU Tools have been installed using the instructions available with the download, you must create the following symbolic links:

- `ln -s /usr/samples/oem_crwriters/burn_cd_gnu /usr/sbin/burn_cd`
- `ln -s /usr/samples/oem_crwriters/mkrr_fs_gnu /usr/sbin/mkrr_fs`

Important Considerations

Backups to a CD or DVD device have their own caveats to consider. Such as:

Space

The creation of backups to CD or DVD devices requires large amounts of free space on your system. You will need to ensure that you have enough space available to perform this process before beginning. There is a flag on the `/usr/sbin/mksbcd` command that will allow the process to estimate the required amount of free space without actually creating the CD or DVD and backup image. However, below are the guidelines to use for determining if you have enough free space on your system This process will create 3 separate file systems for this process.

- The **backup_image** is generated to a file system named by default `/mksbcd/backup_image`. The size of this file system must be equal to the size of your backup. For example: If you are backing up rootvg only, and you have a 4 GB root volume group, this file system will have to be 4 GB in size. Likewise, if you are backing up rootvg and datavg, where rootvg is 4 GB and datavg is 7 GB, this file system will have to be 11 GB in size.
- The **cd_fs** is used as a staging area to create and build boot images, additional software needed for cloning to alternate architectures, software that you choose to optionally install onto the destination system, and portions of the backup image as it is split into media sized pieces. The default file system created is `/mksbcd/cd_fs`. The size of this file system must be equal to the size of your media. For example: If you are using 4.5 GB DVD-RAM media, this file system would have to be 4.5 GB. Likewise, if you are using 9.1 GB DVD-RAM double sided media, this file system would still only be 4.5 GB as it is only equal to one side of the media since only one side of the media can be burned at a time.
- The **cd_image** file system is also called the Rockridge file system since there is where the Rockridge image (iso image) is stored while the CD or DVD burn is in progress. The image in this file system is created from the **cd_fs** contents. The default file system created is named `/mksbcd_cd_image`. This size of this file system must be equal to the size of your media. For example: If you are using 4.5 GB DVD-RAM media, this file system would have to be 4.5 GB. Likewise, if you are using 9.1 GB DVD-RAM double sided media, this file system would still only be 4.5 GB as it is only equal to one side of the media since only one side of the media can be burned at a time.

Limitations

DVD Devices: AIX states that only the CHRP platform supports booting from DVD devices. We have tested booting a 7043-43P (RSPC) from DVD extensively in our testing. Therefore, we will support SysBack DVD boot and install for all SysBack product related issues. However, if the issue becomes an inherent incompatibility or functionality issue between the device, AIX, or rspc firmware that is not supported by the AIX or HW teams, then our support stops there. With this in mind, use DVD devices with SysBack on RSPC platforms at your own discretion.

CD Devices: All 3 platforms, rs6k, rspc, and chrp support booting from CD devices. ****KNOWN BOOT ISSUE WITH CHRP PLATFORM**** At the time of this feature's original creation, there was a known issue with the GNU software not directly supporting the boot of the CHRP platform. The firmware that locates the CHRP boot image in the CD file system is case sensitive. It looks for the boot image filename in lower case. However, the GNU software creates the file name in upper case in the directory structure and the beginning of the file system.

If the CD were to be mounted manually, the names will appear in lower case; however, the firmware still sees them in uppercase and can't file the needed file. You CAN still boot and install from CD / DVD on a CHRP system, provided that you use this work around OR update to GNU utilities created after August 2002 will ensure that you do not encounter this problem. Work around: When booting a CHRP machine, at some point you will hear several beeps followed by a short piece of music. When you hear the first beeps, press the F8 key (or use 8 and Enter for ascii ttys). You will receive a prompt. At the prompt, type the following:

```
boot cdrom:\PPC\CHRP\BOOTFILE.EXE
```

The system should then boot from the CD.

Media

Any type of media (blue vs. gold, and multiple write) is supported. However, testing proves that the better the quality of the media (usually the more expensive media) yields better results with the writing, reading, and booting. Therefore, just as with tape media, the reliability of your backups depends greatly on the quality of your media. Refer to your individual vendor's specifications for information on media suggestions and requirements.

Speed

Please be aware that data transfer rates are inherently slower on DVD and CD devices than most tape devices. Do not expect to achieve the same high speed / performance backups to these devices. In fact, there is nothing in SysBack's design that can be modified to increase or decrease performance. It is completely a result of the individual device used and other system performance issues (like paging, memory etc.). Refer to your individual vendor's specifications to estimate approximate data transfer rates and for any media requirements. Remember however that those specifications are usually quoted as best case and may be in fact lesser than estimated when you are in your actual environment.

Initiating the Backup

Backing up to CD or DVD is different than traditional SysBack backups. Only one backup type to these devices is allowed, the Full System (Installation Image) backup, which is usually generated by the **/usr/sbin/sysback** command. The Full System (Installation Image) backup is the only SysBack backup from which you can boot and install a system. It allows for only a root volume group OR a rootvg and all non-root volume groups backup. However, this backup image to CD or

DVD is not created using the usual **/usr/sbin/sysback** command. Instead, you will use the **/usr/sbin/mksbcd** command. This command has numerous options to customize it to the needs of your environment. Therefore, you may opt to use the SysBack SMIT Menus instead. If you would like to create your CD or DVD backup using the SMIT Menu, you would access the following progression of menus:

```
root@lasher> smitty sysback      Backup & Recovery Options
Backup Options                  Backup the System to CD/DVD
```

All of the SysBack Full System backup options that are available to you when using tape or network backups are still available to you for CD / DVD backups. The SysBack Backup Scripts and Schedules features do not support this backup type. Also, the pull backup feature can not be used with this backup type.

SysBack's ability to support multi-volume backups is supported with the new CD / DVD support.

Initiating a Restore

Restoring data from a SysBack created CD or DVD is no different than restoring data stored on tape.

The same options for restoring portions of data are still available:

- Non-rootvg volume group level
- File system level
- Logical volume level
- File or directory level

The **/usr/sbin/remakevg** command will read CD and DVD media backups and allow you to recreate volume groups, file systems, or logical volumes in the same manner as if the data was stored on tape or in file images. You may also use the same SMIT menu restore options as well.

If you would like to create your CD or DVD backup using the SMIT Menu, you would access the following progression of menus: root@lasher> smitty sysback

```
Backup & Recovery Options      Recreate Volume Groups, Logical
Volumes, or File systems
```

or

```
root@lasher> smitty sysback      Backup & Recovery Options
Restore Data from a Backup
```

SysBack's ability to support multi-volume restores is also supported with the new CD and DVD support.

Boot and Installation

You may boot and install from CD / DVD just as you would with tape using SysBack. You can also boot from CD / DVD and perform a network install as well. Essentially, the CD / DVD devices may be used in any boot / restore / install combination. Consider the following combinations:

Table 5-1. Boot and Install Combinations

Boot Device	Install Device	Post Install Device Support Device
CD / DVD	CD / DVD ⁴	CD / DVD ³
CD / DVD	Tape	CD / DVD ³
CD / DVD	Network	CD / DVD ³
Tape	Tape	CD / DVD
Tape	CD / DVD	CD / DVD
Tape	Network ¹	CD / DVD
Network	Network	CD / DVD
Network	Network	NIM LPPSOURCE ²
Network	Tape	CD / DVD
Network	Tape	NIM LPPSOURCE ²
Network	CD / DVD	CD / DVD
Network	CD / DVD	NIM LPPSOURCE

1. When creating the SysBack backup tape, the `-N <nettype>flag` must be used in order to ensure that the network adapter can be configured to perform the network install. In SMIT, this flag equates to the **Network install support to include** field.
2. A NIM LPPSOURCE may only be a source to obtain post installation device support filesets when a SysBack NIM Resource Network Boot is performed. This option is not available to the SysBack Classic Network Boot.
3. The CD/DVD media used for the system boot does not have to be the same media as what contains the Post Install device support filesets. For example, you could boot from SysBack backup and install device support from an AIX product CD. Also, if using two different discs, they may be used in the same, or different, devices. For example, the boot CD / DVD may be in `/dev/cd0` and the post install fileset support media may be in `/dev/cd1`.
4. The CD / DVD media used for the system boot does not have to be the same media as what contains the backup image to be installed. For example, you could boot from one SysBack backup and install from a different SysBack backup. Also, if using two different discs, they may be used in the same, or different, devices. For example, the boot CD / DVD may be in `/dev/cd0` and the installation image CD / DVD may be in `/dev/cd1`. Furthermore, SysBack will prompt you to change media as appropriate when the same device is specified for the install device and the Post Install fileset support device.

Table 5-2. Media Prompts

Install Device	Post Install Device Support Device	CD / DVD	Result
<code>/dev/cd0</code>	<code>/dev/cd0</code>	Same	Media change not required
<code>/dev/cd0</code>	<code>/dev/cd0</code>	Different	Prompts for media change
<code>/dev/cd0</code>	<code>/dev/cd1</code>	N/A	Media change is not required

SysBack checks the media for the appropriate structure and volume number to determine if the media in the device has the Post Install Device support located on it. In the second scenario above, the media may be different simply because the

install processing completed, and it is possible that you have the 3rd CD or DVD of a multivolume backup loaded. If you created the SysBack backup with the `-s package_source_dir` flag, this Post Install fileset support is located on the first CD or DVD of the backup series. Hence, you will be prompted to load the 1st CD or DVD from the backup series, or an AIX product CD. The Post Install Device support fileset CD or DVD can be the same CD or DVD as what contains the SysBack backup provided that you created the backup with the necessary flags on the `/usr/sbin/mksbcd` command. The SysBack features that allow user defined customized scripts to be automatically executed during the installation process are supported with the CD or DVD devices.

Command Syntax and SMIT Menus

```
mksbcd <-----flags/options-----> vg1 vg2... vgN
```

Note: rootvg is included by default

STANDARD FLAGS:

-f device

Specify CD / DVD device in the form of `/dev/cd0`. This flag is required.

Note: The device specified with this flag can not be the same device specified when the optional `-s pkg_source_dir` is used. If the device is located on a remote host, you must also specify either

The SMIT menu field equivalent to this flag is: Device Name.

-T C|D

Specify the device / media type. C represents CD media and D represents DVD media. Select one. If this flag is not specified, the process will attempt to determine the type of media based on the device specified with the `-f device` flag. This flag is optional.

The SMIT menu field equivalent to this flag is: Media Type?.

-B Creates a Boot only CD / DVD. No backup data will be generated. This flag is optional. The SMIT menu field equivalent to this flag is: Create a Boot only CD/DVD?

-D Sets the environment variable `SBDEBUG=1` to enable debugging of SysBack programs. This flag is optional.

The SMIT menu field equivalent to this flag is: Debug Output?.

-e Estimates the space needed only. This is like the "Preview Only" option with the AIX `installp` command. This flag is optional.

The SMIT menu field equivalent to this flag is: Estimate Space Needed?.

-z size Specify the media size in MB to override default values. Default CD size is 650MB. Default DVD size is 4188 MB (4.09 GB). If the size of your media is double sided, only specify the size of one side of the media, not the total aggregate. This flag is optional.

The SMIT menu field equivalent to this flag is: Media Size.

-G rs6k|rspc|chrp|all

Specify the platform type of the system where the CD / DVD will be utilized. Select one or more options. This flag is optional. If you are creating the CD / DVD on the system where it will be used to boot and install, it is not necessary to specify this flag as the process will default to

the current platform type. For example: If you were creating this CD / DVD on an F50, it would be created to support the CHRP platform. If you are creating the CD / DVD to support this system and a second type of system, such as the default CHRP and also for an RSPC system, you would specify `-G "chrp rspc"` This option requires that all of the device and kernel support required to boot both platforms be installed onto the system creating the CD / DVD. Failure to have all of the needed support installed will not cause the backup and CD / DVD creation to fail. Instead, it will cause the boot to fail when booting from a platform different than where the CD / DVD was created. Optionally adding the `-s pkg_source_dir` along with this `-G` combination will allow you to place this device support for both platforms into the CD / DVD image in order to be utilized as Post Install device support. This would be useful when you want to boot from this CD / DVD which has all needed device support, but install from a backup (tape, CD, DVD, file) that does not have all of the needed support in the backup image. Selecting `-G all` creates a CD / DVD that may be used to boot any system and requires the use of the `-s "pkg_source_dir"` flag which provides all device support to be built into the boot images allowing this to be true. You will also be able to utilize this media as Post Install device support.

Note: Specifying this option will perform an `installp` command against the `pkg_source_dir` and installs those filesets onto this system. Also, this support is placed onto the CD / DVD for use as Post Install device fileset media.

The SMIT menu field equivalent to this flag is: Platform type(s) for CD/DVD boot image

- S** Stops the `/usr/sbin/mksbcd` command before writing to media without removing the final CD image. This leaves you with a final Rockridge Image that may be burned to CD / DVD at a later time. The `backup_image` file system and the `cd_fs` file system will be removed leaving only the `cd_image` file system with the Rockridge Image (iso). If you select this option, you will have to manually burn the image to CD / DVD yourself using the GNU `burn_cd` function instead of using SysBack. This flag is optional.

The SMIT menu field equivalent to this flag is: Create the CD/DVD now?.

-r cd_fs

Specify a previously created `cd_fs` file system that was not removed by a previous `mksbcd` process. Specifying this flag simply directs `mksbcd` to build a new Rockridge Image from this file system and burn the existing backup image to CD / DVD. This flag is optional.

The SMIT menu field equivalent to this flag is: Create Rockridge Image from Previous `cd_fs`.

-m backup_image

Specify an existing `backup_image` file system that contains a single, previously created backup image. The `mksbcd` command will then use this image rather than running a new backup during the `mksbcd` process. Do not specify the `-M backup_image` when using this flag. The SysBack backup utilized with this flag had to have been originally backed up to a file using the `/usr/sbin/sysback` command AND have used the `-2`, `-z cdsizes`, and `-Z maxsize` command flags. This flag is optional.

The SMIT menu field equivalent to this flag is: Existing Backup Image.

-s pkg_source_dir

Specify the device or directory containing AIX device and/or kernel support filesets in the bffcreate format for use in either creating boot images or for use as Post Install Device support. This flag is required with the -G allflag and optional with any other -G flag combination. See the -G flag for additional details.

The SMIT menu field equivalent to this flag is: Location of Software Packages to copy to CD/ DVD.

-l package_list

Specifies a file that contains a list of additional software packages that will be stored in the **/usr/sys/inst.images** subdirectory of the cd_fs file system. The -l flag requires the use of the -s package_source_dir as these packages will be copied from that file system or device. This would be useful when there are AIX filesets that you would like to have installed, but are not considered required device or kernel support filesets. You may also store other third party software product that you would like to be automatically installed.

The SMIT menu field equivalent to this flag is: File with list of packages to copy to CD/DVD.

-c termdev

Specify this flag to indicate the name of a terminal device on which to display volume prompt messages for multi-volume backups. This may be used for local or remote backup volume prompting. Example device names: /dev/tt0 (ASCII Terminal) /dev/pts/1 (Usually a Window in an AIXwindows environment.) /dev/console (System console) This flag is optional.

The SMIT menu field equivalent to this flag is: Device name for remote volume prompt.

WORKSPACE FLAGS:

-M backup_image

Specify the name of an existing file system to be used in place of the default backup_image file system. You must ensure that there is enough space in this file system as outlined in the section entitled "Space" on page 5-2. If this flag is not specified, the default backup_image file system created is **/mksbcd/backup_image**. If there is not enough space in this file system, the mksbcd command will enlarge the file system with the AIX **/usr/sbin/chfs** command to make it large enough. If the chfs command fails, then so will mksbcd. Also, this file system will not be automatically removed by the mksbcd command. However, it's contents will be removed unless you specify the -R M flag. This flag is optional.

The SMIT menu field equivalent to this flag is: File system to store Backup Image.

-C cd_fs

Specify the name of an existing file system to be used in place of the default cd_fs file system. You must ensure that there is enough space in this file system as outlined in the section entitled "Space" on page 5-2. If this flag is not specified, the default cd_fs file system created is **/mksbcd/cd_fs**. If there is not enough space in this file system, the mksbcd command will enlarge the file system with the AIX **/usr/sbin/chfs** command to make it large enough. If the chfs command fails, then so will mksbcd. Also, this file system will not be automatically removed by the

mksbcd command. However, it's contents will be removed unless you specify the -R C flag. This flag is optional.

The SMIT menu field equivalent to this flag is: File system to store CD / DVD file structure.

-I cd_image

Specify the name of an existing file system to be used in place of the default cd_image file system. You must ensure that there is enough space in this file system as outlined in the section entitled "Space" on page 5-2. If this flag is not specified, the default cd_image file system created is **/mksbcd/cd_image**. If there is not enough space in this file system, the mksbcd command will enlarge the file system with the AIX **/usr/sbin/chfs** command to make it large enough. If the chfs command fails, then so will mksbcd. Also, this file system will not be automatically removed by the mksbcd command. However, it's contents will be removed unless you specify the -R I flag. This flag is optional.

The SMIT menu field equivalent to this flag is: File system to store final CD/DVD image.

-R CMI

Specify this flag when you do not want the mksbcd process to remove one or more of the default created file systems. Specify one or more of the following combinations:

C Do not remove the cd_fs file system M Do not remove the backup_image file system I Do not remove the cd_image file system

This can be specified as -R CMI or -R "C M I". This flag is optional.

The SMIT menu field equivalent to this flag is: Do not remove the final CD images.

-V vgroup

Specify this flag when you do not want the default backup_image, cd_fs, and cd_image file systems created in the rootvg volume group. This only applies to locally created file systems. This flag is optional.

The SMIT menu field equivalent to this flag is: Local Volume Group for creation of file systems.

-F vgroup

Specify this flag when you do not want the default backup_image, cd_fs, and cd_image file systems created in the rootvg volume group. This applies to creating these file systems on a remote system and would only be specified in conjunction with the -H host or -h host flags. This flag is optional.

The SMIT menu field equivalent to this flag is: Remote Volume Group for creation of file systems.

HOST OPTIONS:

-h hostname

Specify this option when performing backups to a remote CD / DVD device. This will create the backup_image, cd_fs, and cd_image file systems on the local system and the "cd_image" file system on the remote system. You may optionally use the -F vgroup flag to specify which volume group on the remote system in which to create the cd_image file system.

The SMIT menu field equivalent to this flag is: Build Temp Work Space(s) on.

-H hostname

Specify this option when performing backups to a remote CD / DVD device. This will create the backup_image, cd_fs, and cd_image file systems on the remote system. You may optionally use the -F vname flag to specify which volume group on the remote system in which the 3 file systems will be created.

The SMIT menu field equivalent to this flag is: Hostname of CD/DVD Server.

BACKUP COMMAND FLAGS:

- i ID** A backup file ID is used to create a unique file name when writing a backup to a disk file during the mksbcd processing. The default ID contains the current date and time. You may change this field to any value you desire to describe the backup. If you choose an ID that is already in use in the specified directory, you must also choose to **Overwrite existing backup with same ID**, the -O flag, or the backup will fail. This flag is required.

The SMIT menu field equivalent to this flag is: Backup file ID.

- O** If the specified **Backup file ID**, the -i ID flag, is already used to name a backup in the specified directory, you must use this flag to allow the prior backup to be overwritten. Otherwise, you must choose another unique ID or the backup will not continue. This flag is optional.

The SMIT menu field equivalent to this flag is: Overwrite existing backup with same ID?.

- A** This flag may be used instead of using both the **Backup File ID** and the **Overwrite existing backup with same ID** combination to generate a dynamically created backup file id based on the date and time at the command's execution. This option is useful when the mksbcd command is scripted and schedule to run over some interval. This option takes precedence over the **Backup File ID** and **Overwrite existing backup with same ID** options and is particularly useful when scheduling this command in a backup script. This flag is optional.

The SMIT menu field equivalent to this flag is: Dynamically CreatedBackup File ID.

-d description

You may enter in this field any information up to 60 characters. This information does not affect the backup, but is written to the backup volume label and will appear when the volume label is read. You may not use the single quote character (') in this flag. Doing so will result in a syntax error when the backup command is executed. This flag is optional.

The SMIT menu field equivalent to this flag is: User Description.

-E exclude_list

Enter the fully qualified path and file name to represent the exclude list. Specifying a file name without specifying the path name will cause SysBack to look for the exclude list file in the directory **/usr/lpp/sysback**. Leaving this field blank will cause the product to default to **/usr/lpp/sysback/exclude_list**. This flag is optional.

The SMIT menu field equivalent to this flag is: Exclude List File Name.

-g vginfo_file

Specify the name of a previously created LVM information file customized for this backup. See the `/usr/sbin/mkvginfo` command in Appendix A, “Commands”, on page A-1 for more information on customized LVM information files. This flag is optional.

The SMIT menu field equivalent to this flag is: no equivalent, command line only option

-J

When logical volumes are recreated from a backup, you may choose to create them using the exact same physical partitions on the disks on which they currently reside. This is not possible when installing onto a disk of a different size or physical location on the system. Specifying this option will preserve the current mapping of the logical volume, but will also preserve any fragmentation that currently exists. Preserving the partition mapping is generally not useful unless the logical volumes were originally created using partition maps. This flag is optional.

The SMIT menu field equivalent to this flag is: Preserve physical partition mapping?.

-k buffer_size

The buffer size indicates the amount of data that is written to the output device in a single output operation. Using a buffer size that best optimizes a particular device can have significant performance advantages.

Note: The larger the buffer size, the more memory will be used by the system during the backup.

The SMIT menu field equivalent to this flag is: Buffer size (in Kbytes).

-p

Specifying this option will cause the data to be compressed by this system prior to writing to the backup device. You should not compress data if the device you are writing to has built-in compression capability. However, if you are writing the backup to a remote host and wish to send less data over the network, this option may be useful. However, verify that the output device does not also have compression set. Compressing data will use considerable CPU processing on this system, but will result in less data written to the backup device (in most cases) and usually better backup performance. This flag is optional.

The SMIT menu field equivalent to this flag is: Compress data before writing to media?.

-P

Use this option to create a SysBack Power Backup, a backup in which all file system data is backed up as raw logical volumes. In many cases, this will provide better performance during the backup and during installation from this backup. However, there are some limitations related to customizing the installation. It is not possible to restore select files or directories from this type of backup. This flag is optional.

Note: Logical volumes are backed up in their entirety, even if the file systems are only partially full. Therefore, this could decrease the backup and restore performance.

The SMIT menu field equivalent to this flag is: Create a Power Backup?.

-v

Use this flag to display a list of files as they are being backed up. This flag is optional.

The SMIT menu field equivalent to this flag is: "Report output type".

- x Use this flag to display a progress indicator which shows the estimated total and elapsed time of the backup process. This flag is optional.

The SMIT menu field equivalent to this flag is: Report output type.

- X Use this flag to exclude user data logical volumes. System logical volumes such as boot, paging, and jfs logs will not be affected by this flag.

Note: If a logical volume name exists in the SysBack exclude list, it will not be included in the backup regardless of whether or not this flag is set. This flag is optional.

The SMIT menu field equivalent to this flag is: Include non-JFS logical volumes?.

COMMAND EXAMPLES:

1. To generate a boot only DVD (with no backup data) to the /dev/cd1 device, issue the command:
`mksbcd -B -T "D" -f /dev/cd1`
2. To generate a backup of the rootvg volume group to DVD using the device /dev/cd1, issue the command:
`mksbcd -T "D" -f /dev/cd1`
3. To generate a backup of the rootvg and datavg volume groups to a 5.2 GB (2.6 each side) DVD using the device /dev/cd0, issue the command:
`mksbcd -T "D" -f /dev/cd0 -Z 2662 datavg`
4. To generate a compressed rootvg backup to CD using /dev/cd0, and is bootable by all platform types, and where the AIX product cd will act as the package source media and is loaded into /dev/cd1, issue the command:
`mksbcd -T "C" -f /dev/cd0 -G all -s /dev/cd1`
5. To generate a remote backup, including datavg, to the DVD device on sysback1, and create all of the work space file systems on that remote host in workvg, issue the command:
`mksbcd -T "D" -f /dev/cd0 -H sysback1 -F workvg datavg`
6. To generate a backup of the rootvg volume group to DVD using the device /dev/cd1, and to create the default work space file systems in datavg instead of in rootvg, issue the command:
`mksbcd -T "D" -f /dev/cd1 -F datavg`

Chapter 6. Offline Mirror Backups

SysBack reintroduces a new and enhanced SysBack Offline Mirror Backup capability. This feature had previously been available as a separate option for SysBack 4, but it is now included it at as a base function.

Purpose

Offline Mirror Backup allows you to split AIX mirrors. This allows user and system access to one mirror copy while SysBack accesses the inactive copy for backup operations. With the Offline Mirror Backup feature you can:

- Specify which mirror to split when there is more than one copy
- Specify the work directory for temporary work files
- Specify a **Pre-offline** user defined script which could be used to temporarily quiesce mirrors before they are split. For example, this may be used to temporarily halt a database before splitting mirrors in order to ensure data integrity of the data backed up.
- Specify a user backup script, called a **Backup Command File** which is used to execute the backup. You may also use this script to perform other actions like restarting a database that was halted before the mirrors were split.
- Specify a **Post-offline** user defined script which could be used to perform application tasks or other tasks as desired.
- Perform a **Preview** Offline Mirror Backup that will detect problems that would prohibit mirrors from being split without actually starting the backup.
- List the items to be split at the volume group or the logical volume level
- Perform automated recovery or manual recovery for an interrupted Offline Backup attempt.

Restrictions

Below is the list of restrictions to the SysBack Offline Mirror backup process:

- The Offline Mirror backup process can not backup data in JFS2 file systems at this time due to an AIX limitation with the `/usr/sbin/chfs` command. Once support for JFS2 has been added, SysBack will consider making the necessary updates to support JFS2 at that time.
- When backing up data in file systems, unlike previous versions of the Offline Mirror backup feature, the file systems must be mounted in order for the mirrors to be split.
- There may not be any stale partitions in a logical volume specified to be split. This must be rectified before attempting to split the logical volume. Using the Preview option on the Offline Mirror backup process is a simple way to identify stale partitions. Then, you may use native AIX command `/usr/sbin/syncvg` command or the SysBack SMIT Menu Resynchronize Stale Partitions for a Volume Group.

Performing an Offline Mirror Backup

The Offline Mirror Backup process is comprised of two pieces. This first piece is the Offline Mirror process which:

- Splits the AIX mirrors
- Calls the **Backup Command File**
- Re synchronizes the AIX mirrors after completion of the Backup Command File.

The second piece of the Offline Mirror Backup is the actual data backup process which is used to execute the backup. You may also use this script to perform other actions like restarting a database that was halted before the mirrors were split.

Note: It is not necessary to halt your database for the mirror re synchronization process at the end of the Offline Mirror Backup. However, it is still highly recommended that you halt your database while the mirrors are being split and the data backup begins.

The SysBack backup commands in the Backup Command File can backup data that is mirrored and data that is not mirrored. For example: If you specify to split all of the mirrors in datavg the Offline Mirror Backup process, you may also include rootvg and appvg in the same backup process even if they are not mirrored. The SysBack backup command used in the Backup Command File will take the appropriate actions to backup the split mirrors as appropriate, and the default resources when it isn't.

Note: The boot logical volumes and paging spaces do not have to be mirrored in order for the Offline Mirror Backup to process successfully. In most cases, it is not advisable to mirror them. The SysBack Offline Mirror Backup process will not attempt to split their mirrors. However, if you have specified a JFSLOG to be split and backed up, the JFSLOG must be mirrored.

To initiate an Offline Mirror backup:

1. Log in as the root user.
2. Type **smitty sysback** and press Enter.
3. Select **Offline Mirror Backup Options** and press Enter.

The following menu will display:

Offline Mirror Backup Options

Move cursor to desired item and press Enter.

Maintain Backup Command Files
 Perform an Offline Mirror Backup
 Maintenance Utilities

F1=Help
F9=Shell

F2=Refresh
F10=Exit

F3=Cancel
Enter=Do

F8=Image

Figure 6-1. The Offline Mirror Backup Options Menu

4. Select **Perform an Offline Mirror Backup** and press Enter.
5. If there are predefined Backup Command File scripts, select the script to use for the backup on the Device Selector screen. However, if there are no predefined Backup Command Files, choose the option (none) at the Device Selector screen and press Enter.

The following screen is displayed:

Perform an Offline Mirror Backup

Type or select values in entry fields.
 Press Enter AFTER making all desired changes.

	[Entry Fields]	
Preview Only?	no	
BACKUP COMMAND SCRIPTS		
Pre-offline Script	<input type="text"/>	/
Backup Command Script	<input type="text"/>	+ /
Post-offline Script	<input type="text"/>	+ /
Mirror Copy	2	+
Force Continue on Errors?	no	+
Verbose?	yes	+
Sleep (seconds) between each mirror separation	<input type="text"/>	+
Logical Volume List	<input type="text"/>	+
Volume Group List	<input type="text"/>	+

F1=Help
F5=Reset
F9=Shell

F2=Refresh
F6=Command
F10=Exit

F3=Cancel
F7=Edit
Enter=Do

F4=List
F8=Image

Figure 6-2. The Perform an Offline Mirror Backup Menu

6. After making the desired selections, press Enter. The Offline Mirror process will begin by splitting the specified AIX mirrors. Once all of the mirrors are split, the process will stop and leave you at a shell prompt. You will enter your backup command at this shell prompt.

Note: If you chose to specify a Backup Command File instead, that script will be executed rather than a command prompt appearing.

7. Once the backup command completes, you will be returned to the shell prompt.
8. Type the `exit` command to exit the shell. The Offline Mirror process will then begin to re synchronized the stale mirror partitions.

Note: If you had specified a Backup Command File script, once the script exits, the Offline Mirror process will automatically continue with the mirror re synchronization.

The high level process flow for an Offline Mirror Backup is as follows:

- Checks AIX mirror rules for each logical volume specified to be taken offline.
- Checks to make sure that each file system is mounted for each logical volume specified for the mirror split.

Note: This check does not apply to raw logical volumes.

- Checks to make sure that the `jfslog` is mirrored for each file system being taken offline.
- Checks to ensure that no JFS2 file systems have been specified.

Note: JFS2 file systems are not supported for the offline mirror backup process. However, they may be included in the actual backup command executed at either a shell prompt or by a Backup Command File

- Checks to ensure that all specified logical volumes are actually mirrored.
- Checks to ensure that there are no stale physical partitions.

Note: If stale partitions are found, the process will offline mirror process will issue a warning message and the logical volume containing stale partitions will not be split. The backup process will continue. You must use the `/usr/sbin/syncvg` command to re synchronized the stale. You may also use the SysBack SMIT fast path smitty `sbom_syncvg` to perform this action.

- Display a list of all of the warning and error messages for all logical volumes that failed the above checks.

Note: Logical volumes of type boot, sysdump or paging are not taken offline. These are not considered errors, but will issue a warning if specified.

- Display a list of all logical volumes that passed the offline mirror rules
- If you did not use the Force to Continue on Errors option and there were errors reported, the Offline Mirror process would terminate at this point.
- If you specified a Pre-Offline script, it would be run at this point.
- Specified raw logical volumes are taken offline and split using the `/usr/sbin/chlvcopy` command.
- Specified file systems and their respective logical volumes are split using the `/usr/sbin/chfs` command. They are split in alphabetical order by mount point. This creates a temporary mount point called `/sbom/your_filesystem`.
- If you specified a Backup Command File, then it would be run at this point. If you did not, you will be placed at a command prompt where you may issue your backup command.
- The backup process runs.
- Once the Backup Command File script exits, or the command prompt is exited, the Offline Mirror process will begin to re synchronized the mirrors.
- The split logical volumes are re synchronized.

- The temporary split file system mount points are unmounted and removed in reverse alphabetical order by mount point. This causes the underlying logical volumes to be automatically re synchronized.
- All temporary work and status files are removed.

Maintaining Backup Command Files

SysBack provides a SMIT menu interface to assist you with creating your Backup Command Files. These files are simply backup scripts. The SMIT menu interface for maintaining these scripts looks like the SMIT menus for each of the five backup commands. Therefore, you do not have to know the exact SysBack backup command syntax in order to create a script. However, for those who are experienced with creating scripts, there is also an interface to create a generic script. In any backup script that you create, you may included any number of operations to prepare for the backup. You are not limited to SysBack command usage in the Backup Command Files. Also, you may create your scripts with the text editor of your choice instead of using the SysBack SMIT menu interface.

To create a Backup Command File using the SysBack SMIT menu interface:

1. Log in as the root user.
2. Type **smitty sysback** and press Enter.
3. Select **Offline Mirror Backup Options** and press Enter.

The following menu will display:

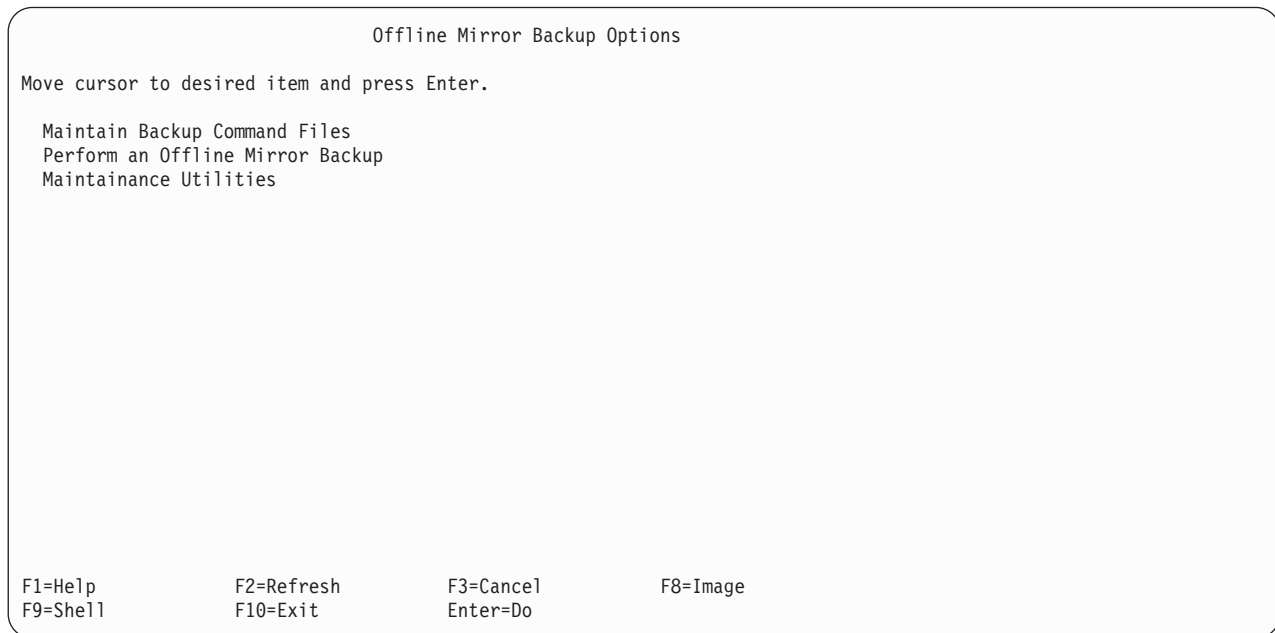


Figure 6-3. The Offline Mirror Backup Options Menu

4. Select **Maintain Backup Command Files** and press Enter.

The following menu will display:

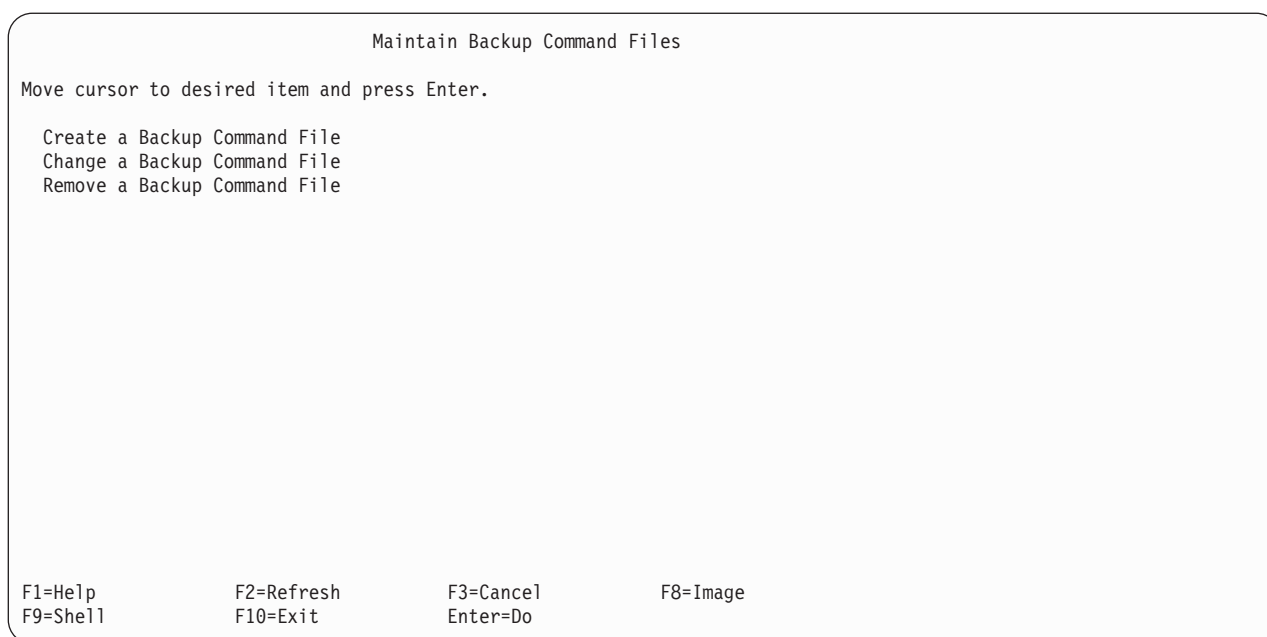


Figure 6-4. The Maintain Backup Command Files Menu

5. Select **Create a Backup Command File** and press Enter.
 The following screen will display:

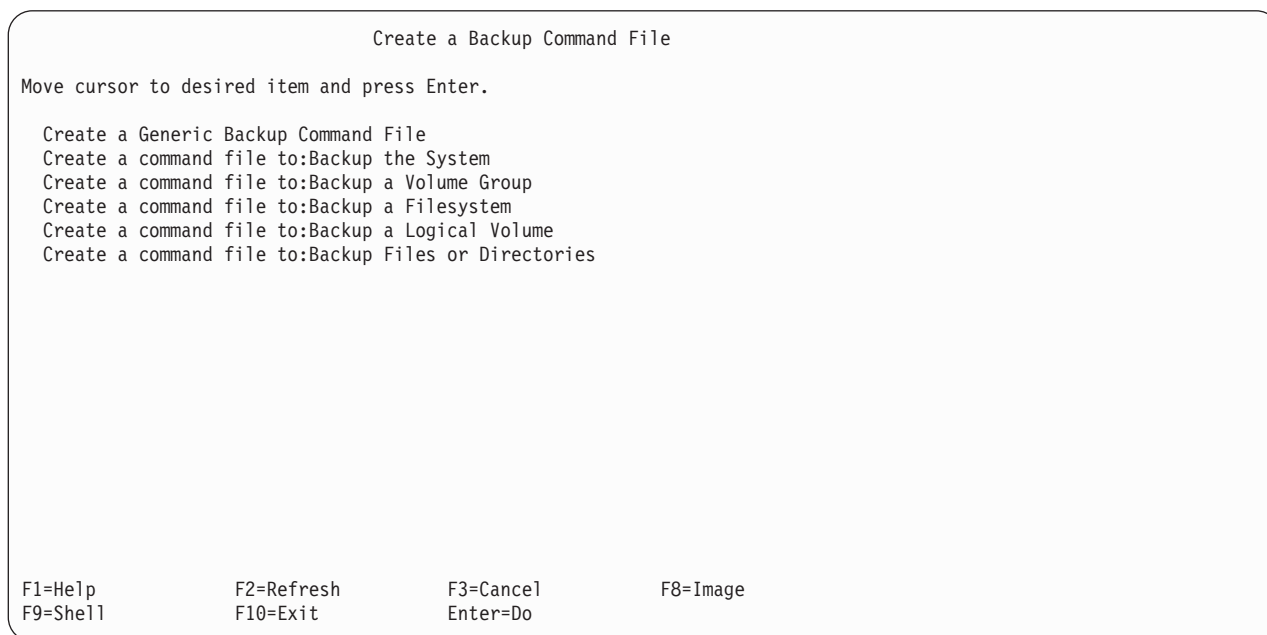


Figure 6-5. The Create a Backup Command File Menu

6. Select **Create a command file to: Backup the System** and press Enter.
 The following screen will be displayed:

Create a command file to: Backup the System

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

[TOP]

Backup Command File Name	[sbom_backup]
File Description	[System Backup]
-----command options-----	sysback
Backup Data hostname	[]
Device Name	[/dev/rmt0]
Create a Power Backup?	No
Report output type	File List
Platform/kernel type for tape boot image	rspec/MP
Network install support to include	
Compress data before writing to media?	No
User Description	[]
Buffer size (in Kbytes)	[64]
Preserve Physical partition mapping?	No
Device name for remote volume prompt	[]
[MORE]	

F1=Help
F5=Reset
F9=Shell

F2=Refresh
F6=Command
F10=Exit

F3=Cancel
F7=Edit
Enter=Do

F4=List
F8=Image

Figure 6-6. The Create a System Backup Script Menu

7. Input the desired values for each field and press Enter.

Scripts created using the SysBack SMIT menu interface will be located in the **/usr/lpp/sysback** directory unless you provide an alternate, fully qualified path. Below is an example of a Full System backup script created using the SMIT menu interface:

```
#!/bin/ksh
# Command filename:
/usr/lpp/sysback/sbom/sbom_sys                                     #
Description:      System Backup
sysback -R /sbom -h "remote.host.ibm.com" -f "/backups/my_host" -I "031803"
-i -p
-o
exit $?
```

The scripts created are not checked for valid backup command syntax options.

Maintenance Utilities

SysBack provides options to assist you with the synchronization of stale partitions that are prohibiting a backup from running and to recover from a failed Offline Mirror backup.

Synchronizing Stale Partitions

SysBack looks for stale partitions for any device whose mirror is specified to be split for backup processing. The AIX mirrors can not be split while stale partitions exist. If the Offline Mirror backup process detects stale partitions, it will display a warning message indicating that this condition was encountered and will not split that logical volume's mirror.

You may attempt to re synchronize stale partitions with the `/usr/sbin/syncvg` command. However, SysBack also provides a SMIT menu interface to assist you with the execution of this command.

To synchronize stale partitions in a volume group:

1. Log in as the root user.
2. Type **smitty sysback** and press Enter.
3. Select **Offline Mirror Backup Options** and press Enter.

The following menu will display:

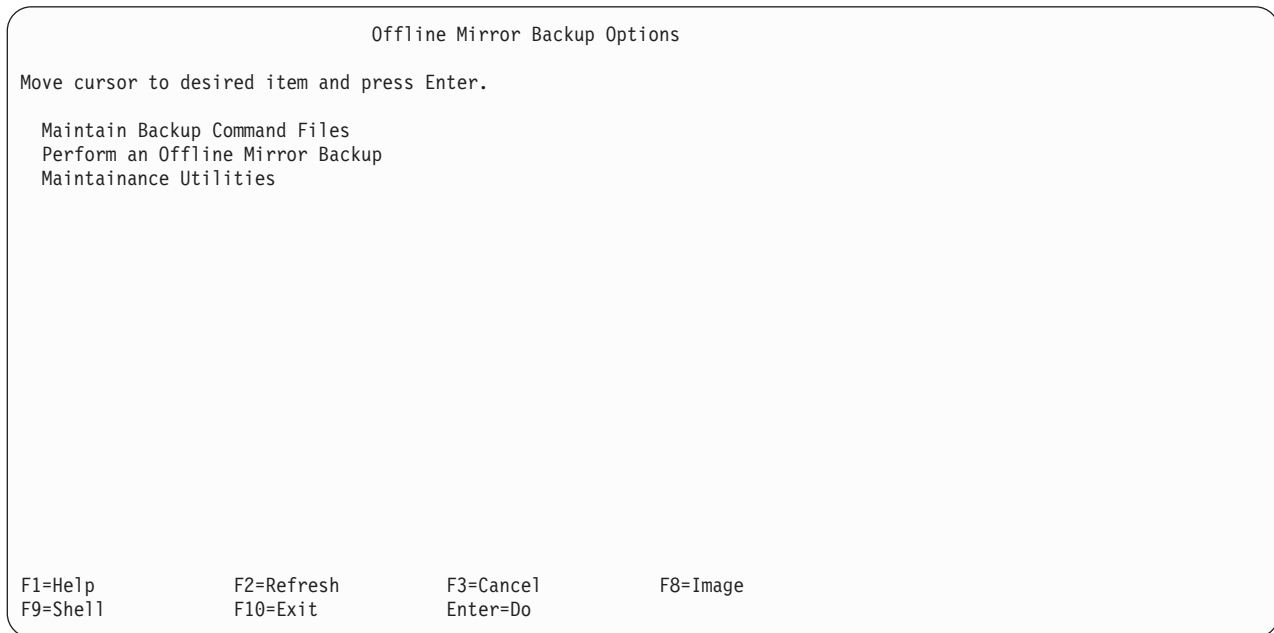


Figure 6-7. The Offline Mirror Backup Options Menu

4. Select **Maintenance Utilities** and press Enter.

The following menu will display:

Maintenance Utilities

Move cursor to desired item and press Enter.

Recover from System Failure during an Offline Mirror Backup
Synchronize Stale Partitions for a Volume Group

F1=Help
F9=Shell
F2=Refresh
F10=Exit
F3=Cancel
Enter=Do
F8=Image

Figure 6-8. The Maintenance Utilities Menu

5. Select **Synchronize Stale Partitions for a Volume Group** and press Enter.
The following menu will display:

Synchronize Stale Partitions for a Volume Group

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

* Volume Group Name

[Entry Fields]

+

F1=Help
F9=Shell
F2=Refresh
F10=Exit
F3=Cancel
Enter=Do
F8=Image

Figure 6-9. The Synchronize Stale Partitions for a Volume Group Menu

6. Enter the name of the volume group with partitions to be synchronized and press Enter.

Note: Before you initiate this process, you should fully understand the implications of running the `/usr/sbin/synchvg` command as well as any restrictions to its use. Please consult your AIX documentation or your technical support contact if you need assistance with this process.

Recover from a Failed or Aborted Offline Mirror Backup

You need to recover when the Offline Mirror Backup process is interrupted and never completes. This could occur when someone or something killed the Offline Mirror backup process before completion. For example, you experienced a system crash while the backup process was running. If you receive the message below when attempting to start a new Offline Mirror Backup process: There appears to be another sbom_backup process running!

and there are no other Offline Mirror backup processes are running, issue the command: `sbom_backup -RF`. You may also use the SysBack SMIT menu interface to perform the recovery.

To synchronize stale partitions in a volume group:

1. Log in as the root user.
2. Type **smitty sysback** and press Enter.
3. Select **Offline Mirror Backup Options** and press Enter.

The following menu will display:

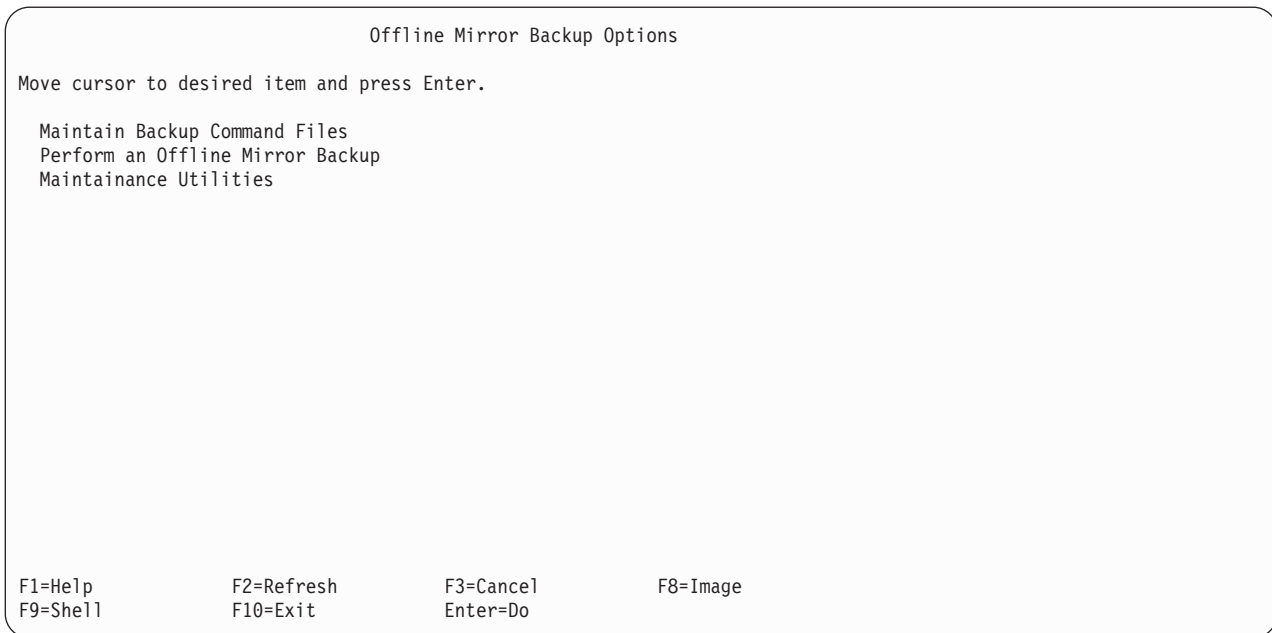


Figure 6-10. The Offline Mirror Backup Options Menu

4. Select **Maintenance Utilities** and press Enter.

The following menu will display:

```

                                Maintenance Utilities

Move cursor to desired item and press Enter.

Recover from System Failure during an Offline Mirror Backup
Synchronize Stale Partitions for a Volume Group


F1=Help      F2=Refresh      F3=Cancel      F8=Image
F9=Shell     F10=Exit       Enter=Do

```

Figure 6-11. The Maintenance Utilities Menu

5. Select **Recover from a System Failure SysBack during an Offline Mirror Backup** and press Enter.

The following menu will be displayed:

```

                                Recover from System Failure during an Offline Mirror Backup

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

                                [Entry Fields]
Force Continue on Errors?      no      +
Verbose?                       yes     +


F1=Help      F2=Refresh      F3=Cancel      F8=Image
F9=Shell     F10=Exit       Enter=Do

```

Figure 6-12. The Recover from System Failure during an Offline Mirror Backup Menu

If this automated recover can not be executed or fails from some reason, please refer to the section “Manual Recovery” on page 6-13 for information on how to manually recover.

Command Syntax and SMIT Menus

`sbom_backup <----- flags/options-----> vgroupname lvname FLAGS:`

- Q** Specifying this option will initiate a validation process of the specified volume groups and logical volumes ensure that the AIX mirrors for these resources can actually be split. This process will generate output that includes the reasons why a specified resource may not have its AIX mirror split, as well as, indicating which of the specified resources did pass the validation process. Additionally, the Offline Mirror backup process will not execute, only validate. It is recommended that you perform this preview operation before attempting to begin your Offline Mirror backup. This flag is optional.

The SMIT Menu field equivalent to this flag is: Preview Only

-p scriptname

Use this option to specify the path and file name of a Pre-offline script that should be executed before the AIX mirrors are split. This flag is optional.

The SMIT Menu field equivalent to this flag is: Pre-offline Script.

-x scriptname

Use this option to specify the path and file name of a Backup Command File script that will be executed after the AIX mirrors are split. This is normally used to perform the actual data backup. If no Backup Command File was specified, you will be presented with a command prompt where you must then manually enter your commands. This flag is optional.

The SMIT Menu field equivalent to this flag is: Backup Command Script.

-P scriptname

Use this option to specify the path and file name of a Post-offline script that will be executed after the AIX mirrors are re synchronized. This flag is optional.

The SMIT Menu field equivalent to this flag is: Post-offline Script.

- c 2|3** Specify the AIX mirror copy that you would like to be split off for the Offline Mirror backup process. The supported values are 2 or 3. The default value is 2. This flag is required.

The SMIT Menu field equivalent to this flag is: Mirror Copy.

- F** Use this option to indicate that you wish the Offline Mirror backup process to continue even if errors are encountered. An example of this might be that the specified Pre-offline script failed to execute. Another example might be that you specified a logical volume to be split but that the AIX mirror can not be split for some reason. Without specifying this flag, the Offline Mirror backup process would terminate. This flag is optional.

The SMIT Menu field equivalent to this flag is: Force Continue on Error.

- v** Use this option to display all status / progress messages during the Offline Mirror backup process. This flag is optional.

The SMIT Menu field equivalent to this flag is: Verbose.

-t dirname

Use this option to specify the directory name to store temporary work files created by the Offline Mirror process. If no directory is specified, the **/tmp** directory will be used. This option does not apply to the temporary work files generated from the actual SysBack backup command. This flag is optional.

The SMIT Menu field equivalent to this flag is: Work Directory.

- R** Use this flag to recover from an interrupted Offline Mirror backup process.

It may be used in combination with the `-F` and `-v` flags only. This SMIT menu equivalent is the **Recover from System Failure during an Offline Mirror Backup** menu. Use this flag only when you receive the message There appears to be another sbom_backup process running! when attempting to initiate an Offline Mirror backup process. You will receive this message only when someone or something killed a previous Offline Mirror process. Confirm that there are in fact no other Offline Mirror processes running before utilizing this flag to cleanup and reset the aborted process.

lvname vgroup

- Specify a list of logical volumes that should have their AIX mirrors split by this Offline Mirror backup process. This list is not required when specifying a list of volume groups. However, both a list of volume groups and logical volumes may be specified simultaneously. If a logical volume is included in a listed volume group do not specify it again individually. File system names may not be specified. Instead, you must specify the underlying logical name.
- Specify a list of volume groups that should have their AIX mirrors split by this Offline Mirror backup process. This list is not required when also specifying a list of logical volumes. However, both a list of volume groups and logical volumes may be specified simultaneously.

COMMAND EXAMPLES:

1. To split the mirrors in the sbvg volume group and use the Backup Command File named **split.vg.backup** to perform the backup, use the command:

```
sbom_backup -x split.vg.backup sbvg
```

2. To split the mirrors of the volume group **sbvg**, along with the mirrors for the logical volumes **lv27** and **testlv** in **datavg**, forcing the process to continue if errors are encountered, and displaying the output to the screen, use the command:

```
sbom_backup -F -v sbvg lv27 testlv
```

Note: If you do not specify a Backup Command File with the `-x` flag, you will be placed at a command prompt to allow you to input the backup commands of your choice. Once the backup commands complete, type **exit** at the command prompt to allow the Offline Mirror process to begin re synchronizing the split mirrors.

3. To recover from an interrupted Offline Mirror backup process, such as when the process was terminated inadvertently. issue this command to clean up and re synchronize mirrors:

```
sbom_backup -R
```

Manual Recovery

If you need to recover from a failed Offline Mirror backup attempt, but the automated recovery process was unsuccessful, you will need to manually recover from the failed backup attempt.

To recover manually, you would do the following:

1. Obtain a listing of all of the active volume groups on your system using the **lsvg -o** command.
2. Obtain a listing of all of the logical volumes in each volume group using the **lsvg -l vgroup** command.

3. Repeat step 2 for each volume group identified in step 1.

Once you have obtained the above information, we are looking to identify any logical volume matching these traits:

- Logical volume names like: lvnameL (capital letter *L* at the end of the logical volume name). For example: sb1vL
- Logical volume names like: lvnamecopy00 (the string *copy00* at the end of the logical volume name). For example: sbfscopy00.
- A logical volume with a state of:
 - open??????
 - closed??????
- A mount point named like: /sbom/directory (has a parent directory of /sbom). For example: /sbom/sbfs2.
- Logical partitions (LPs), physical partitions (PPs), or physical volumes (PVs) will have values of zero.

Once you have compiled the list of all of the logical volumes and file systems that match the above criteria then perform the following to steps to re synchronize your mirrors and clean up the system.

- For any file system that had a parent directory of /sbom, execute the following commands:

```
umount /sbom/filesystem rmfs /sbom/filesystem
```

Note: If there are multiple file systems affected, you must perform this process by unmounting them in reverse alphabetical order.

- For any affected logical volume that also had a mount point of N/A, run the following command:

```
chlvcopy -fB "lvname
```

- Repeat the above operation until all affected file systems and logical volumes are addressed.

This is an example of the output from the **lsvg -o** command.

```
# lsvg -o rootvg sbvg sbvg1 vg00
```

This is an example of the output from the **lsvg -l vgrname** command.

```
# lsvg -l sbvg
```

LV NAME	TYPE	LPs	PPs	PVs	LV STATE	MOUNT	POINT
loglv01	jfslog	1	3	3	open/syncd	N/A	
sb1lv	jfs	10	30	3	closed/syncd	N/A	
sb2lv	jfs	10	30	3	closed/syncd	N/A	
lv07	jfs	3	9	3	open/stale	/sb1fs	
lv05	jfs	3	9	3	open/stale	/sbfs	
lv10	jfs	10	20	2	open/stale	/sbfs/data/directory	
lv11	jfs	10	20	2	open/stale	/sb1fs/data/directory	
sb1lvL	jfs	0	0	0	closed??????	N/A	
sb2lvL	jfs	0	0	0	closed??????	N/A	
lv07copy00	jfs	0	0	0	open??????	/sbom/sb1fs	
lv05copy00	jfs	0	0	0	open??????	/sbom/sbfs	
lv10copy00	jfs	0	0	0	open??????	/sbom/sbfs/data/directory	
lv11copy00	jfs	0	0	0	open??????	/sbom/sb1fs/data/directory	

From the above output, we see that the following file systems and logical volumes are affected and should be removed: File systems: /sbom/sb1fs /sbom/sbfs

/sbom/sbfs/data/directory /sbom/sb1fs/data/directory Logical Volumes: sb1lvL
sb2lvL To remove them in the correct order:

```
# unmount /sbom/sb1fs/data/directory
# unmount /sbom/sbfs/data/directory
# unmount /sbom/sb1fs
# unmount /sbom/sbfs
# rmfs /sbom/sb1fs/data/directory
# rmfs /sbom/sbfs/data/directory
# rmfs /sbom/sb1fs
# rmfs /sbom/sbfs
# chlvcopy -fB sb1lvL
# chlvcopy -fB sb2lvL
```

Chapter 7. Local User Access

When you install SysBack, all users on the local system are, by default, granted access to all backup devices on the system. They are also allowed to create backups in the default directory **/usr/lpp/sysback/bf/local/all**. The following options are used to change user access by adding or deleting the devices or directories that each user can access.

To access the local device or directory access menu:

1. At a command line, type `smit`.
2. Select **IBM Tivoli Storage Manager for System Backup and Recovery**.
3. Select **Configuration Options**.
4. Select **Local User Access**.

You can also access this menu using the fastpath. To do this, type `smit sb_local` at a command line.

The following screen is displayed:



Figure 7-1. The Local User Access Menu

Detailed instructions for each of the selections in the Local User Access menu follow.

Understanding Local User Access Permissions

SysBack provides flexible access for device, directories, and so on. For instance, you can assign specific devices and directories to each user on the system, or assign a device to all users on the system except specific users. Before you assign access, it is important to understand the priority of the permission records and how they are used.

Assume the following records exist:

Users to allow	Users to deny	Devices	Directories
all	greg peter bobby	/dev/rmt0 vdev0	/usr/lpp/sysback/bf/local/all
root		all	usr/lpp/sysback/bf/local/root
alice		/dev/rmt1	

Based on the information above, the following statements are true:

1. Users *greg*, *peter* and *bobby* do not have backup access on this system because they are explicitly denied access under *all* users. You can only deny access to users when defining access for “all” other users. You cannot create a permission record for any users that have been explicitly denied access.
2. User *root* has access to all devices (tape and virtual). User *root* is also provided a disk image file backup option, with the default filename contained in the */usr/lpp/sysback/bf/local/root* directory. You can change the default name of the backup file at backup time, but the file must exist in the */usr/lpp/sysback/bf/local/root* directory or one of its subdirectories.
3. User *alice* has access only to tape device */dev/rmt1*. Because there are no directories defined for backup image files, no disk image backup option is provided to this user.
4. All other users (all users except those explicitly denied and those explicitly defined) are provided access to tape device */dev/rmt0* and virtual device *vdev0*. Those users are also provided a disk image backup option in the */usr/lpp/sysback/bf/local/all* directory. They can back up to only those devices and directories defined in this record.

Also note that, if you remove user *greg* from the list of users denied access, he is automatically provided access under the same record as *all* other users. Likewise, removing user *alice* does not disable access, because she is not explicitly denied, but her permission also defaults to that of *all* users.

Adding or Changing Local User Device/Directory Access

All users on the system are provided access to all of the backup devices on the system when SysBack is first installed. This is accomplished by providing a permission record for a user called *all*. You might not want certain users to have access to all devices and backup directories, so you might want to deny specific users access, or change the device or directory list that specific users are allowed to use. The devices and directories specified when using this option determine the list of backup options that users receive when performing backups using SMIT, and those devices or directories that other SysBack commands, executed at the command line, can read or write to.

If you do not want all users on the system to be granted the same access, remove access to user *all* before setting up access to specific users. This can help avoid confusion in the future.

To add or change device or directory access to local users:

1. From the Local User Access menu, select **Add or Change Local User Device/Directory Access**.

Note: You can also type `smit sb_cfglocaccess` at the command line.

2. Enter the name of the user whose access you want to add or change.

The default entry is *all*. Press Enter to select this entry, change the entry to another user name, or press F4 to list user records previously configured and select a user from the list.

The following screen shows the system default permission record for *all* users on the system:

Add or Change User Device/Directory Access

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

* User name to allow

If all: Users to deny access

Tape or Virtual Devices for backups or "all"

Directory path for backup images

Directory path for network install images

[Entry Fields]

all

[] +

[all] +

[/usr/lpp/sysback/bf/lo> +

[/usr/lpp/sysback/image> +

F1=Help

F2=Refresh

F3=Cancel

F4=List

F5=Reset

F6=Command

F7=Edit

F8=Image

F9=Shell

F10=Exit

Enter=Do

Figure 7-2. The System Default Permission Record for "all" Users

The fields have the following meanings:

User name to allow

The user name entered or selected on the prior screen. You cannot change this field on this screen.

If all: Users to deny access

Default=(blank/none). If you selected to add or change the record for "all" users, enter a list of users, separated by spaces, to be explicitly denied access. In other words, all users except those specified here will be permitted.

Tape or Virtual Devices for backups or "all"

Default=(blank/none). If the specified user is allowed to back up to a tape drive or virtual device, enter the device name or names, separated by spaces. You can also press F4 to list the available tape and virtual devices on the system and select one or more devices from the list using F7.

Enter "all" to provide a backup option for this user for all tape and virtual devices on the system.

Only the devices entered here are displayed on the SMIT menus when the user selects a backup.

Directory path for backup images

Default=(blank/none). If you want to allow the specified user to perform backups to *disk image files*, enter the directory or directories, separated by spaces, that the user can back up to. Press F4 to display a list of backup image directories already selected, or the default

directory of **/usr/lpp/sysback/bf/local/username**. Highlight each entry you want to save and press F7. Press Enter to continue.

When performing any SysBack backup, you are provided a directory backup option for each directory specified. The actual file created in the directory is named according to the information in Chapter 2, "SMIT Overview", on page 2-1.

Directory path for network install images

Default=(blank/none). This field applies only to the "root" user, because only the root user can create a system backup. Enter information in this field only when configuring the "root" user or "all" users if root is not specifically defined.

Enter each directory for which you want to save installation images, each separated by space. Press the F4 key to display a list of installation image directories already selected, or the default directory of **/usr/lpp/sysback/images/local**. Highlight each entry you want to save and press F7. Press Enter to continue.

When performing the option to **Backup the System**, the user is provided a directory backup option for each directory specified. Also, when this or other systems attempt to perform a network installation, all backup images in the specified directories that the client system has permission to read are displayed as network install options.

3. Press Enter to complete this process. Repeat the above steps to grant access to other users.

Listing User Access

Use the **List User Access** option to display a list of all user permission records. The list includes users permitted and denied, along with the devices and/or directories that each user is permitted to access. To list the users:

1. From the Local User Access menu, select **List User Access**.

Note: You can also list users by typing `smit lb_lslocaccess` at a command line.

The list is displayed with no further prompts.

Removing User Access

Use the **Remove User Access** option to remove permission records.

Removing a specific user's permission record does not automatically deny that user access if there is also a permission record defined for "all" users. If a record exists for "all" users, and you want to deny access to a specific user, you must remove the user's permission record, if any, and then add that user name to the list of users to deny using the **Add or Change Local User Device/Directory Access** option.

To remove user access:

1. From the Local User Access menu, select **Remove User Access**.

Note: You can also type the fastpath `smit sb_ucfglocaccess` at a command line.

2. Select a user from the list of users with permission records currently defined.

If a record exists for “all” users, an option for “all” is displayed. If you remove the record for “all” users, all users except those with permission records explicitly defined for them will be denied access.

3. Press Enter to confirm your choice. Doing so removes the selected permission record from the file with no further prompts.

Chapter 8. Remote Services

Remote Services is an optional feature of SysBack that enables a host attached to a network using TCP/IP to read and write backups to and from either tape drives or disks attached to a remote host. This enables a single host to act as a backup server for other hosts on the network that do not have a local tape drive attached.

With Remote Services, a backup server machine can enable specific hosts and users on those hosts to access the local devices or directories. Remote Services also enables client hosts to be installed from a device or disk image file on a network installation server.

To use Remote Services, SysBack must be installed on each host that you want to act as a backup server, as well as each host that backs up its data to the server. TCP/IP must also be installed on each host to use Remote Services functions.

To access the menu for configuration and maintenance of a backup server or client:

1. Type `smit` at a command line.
2. Select **IBM Tivoli Storage Manager for System Backup and Recovery**.
3. Select **Configuration Options**.
4. Select **Remote Services**.

You can also use the following fastpath to access this menu: `smit sb_remote`.

The following screen is displayed:

```
Remote Services

Move cursor to desired item and press Enter.

Server Options
Client Options

F1=Help      F2=Refresh   F3=Cancel    F8=Image
F9=Shell     F10=Exit     Enter=Do
```

Figure 8-1. The Remote Services Menu

This first screen contains two options, one for server configuration and one for client configuration. The following screens show the options for each. Each of these options is described in the sections below.

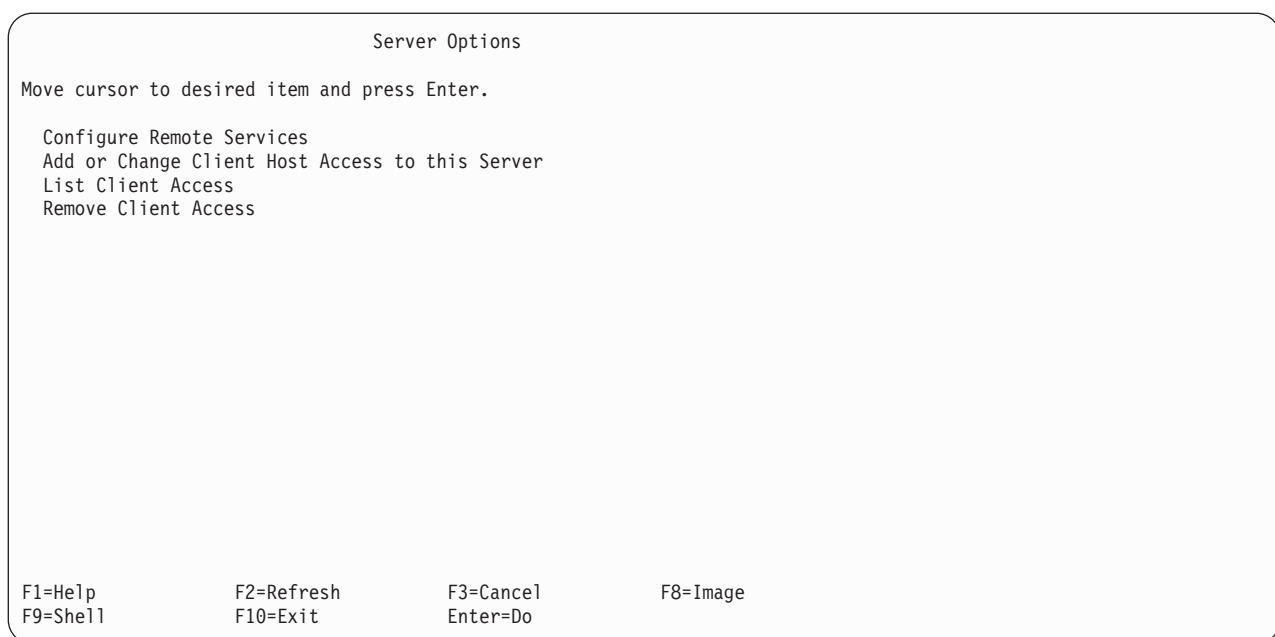


Figure 8-2. Server Options from the Remote Services Menu

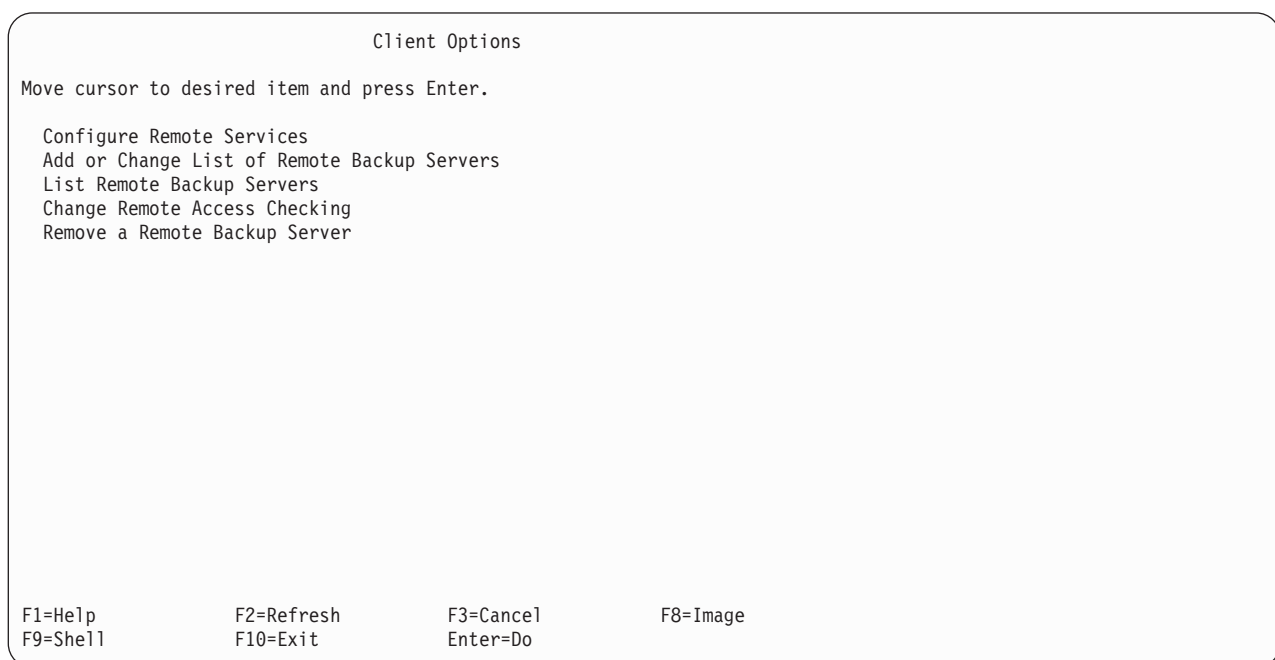


Figure 8-3. Client Options from the Remote Services Menu

Understanding Remote Host and User Access Permissions

SysBack is very flexible as to which hosts, and users on those hosts, can access the devices or directories on the local system, as well as which devices or directories they may access. For instance, specific devices or directories or both can be assigned to all users on all client hosts, or all devices can be assigned to specific users on specific hosts.

The following example describes the permission records and how they are interpreted. Note that this is a complex example. Ordinarily, records are defined for all hosts, or for each specific host, but not both.

Assume the following client host/user records exist:

Host to allow	Hosts to deny	Users to allow	Users to deny	devices	backup directories	network installation image directories
venus		root		all	/usr/lpp/sysback/bf/venus/root	
venus		all	bobby cindy	/dev/rmt1		
all		root		all		/usr/lpp/sysback/images/all
all	mars pluto	all	greg marsha peter	/dev/rmt0 vdev0	/usr/lpp/sysback/bf/all/all	

When a client host attempts to gain access to a server, permission records are checked on the server in the following order:

1. First, the permissions on the server are checked to ensure that the host attempting to gain access has not been explicitly denied access. Hosts denied access are shown only under the record assigned to “all” hosts. If, for example, any user on host *mars* that attempts to perform a backup to this server will receive a message that permission is denied.
2. Next, permission records are searched to ensure that the specific user has not been denied access. Users can be denied access under any record that applies to “all” users. If on any host user *marsha* attempts to gain access, she will be denied access because the host record for “all” hosts explicitly denies access to her. If user *cindy* on host *venus* attempts to gain access, she will be denied because she is explicitly denied access from *venus*. User *cindy* can perform a backup from any other hosts.
3. Assuming the host or user is not explicitly denied access, records are then searched for one matching the specific host and user. In the above example, if the *root* user on host *venus* attempts to gain access, this user will be allowed to backup to all devices and the **/usr/lpp/sysback/bf/venus/root** directory on the server.
4. If the above record does not exist, records are searched for one matching “all” users on the specific host. In the above example, if user *jan* on host *venus* attempts to gain access, she will obtain permission from the record assigned to *all* users on *venus*. She will therefore have access to only device */dev/rmt1* and no backup image directories.
5. Lastly, if none of the above succeed, records are searched for “all” users on “all” hosts. If user *alice* on host *neptune* attempts to perform a backup to the server, she will gain access under this record. She will therefore be allowed to back up to devices */dev/rmt0* and *vdev0* and to backup image directory **/usr/lpp/sysback/bf/all/all**.

Also note that, by removing the record for host *venus* and user *all*, all users on *venus*, except *root*, still have access to the devices and directories defined under the record for *all* users on *all* hosts. Note also that, by removing this record, users *bobby* and *cindy* also have access under *all* users on *all* hosts because they are no longer explicitly denied.

The entry for **network installation image directories** applies only to either the *root* user, or *all* users if the root user is not explicitly defined. This entry determines the directory or directories from which the installation image files will be listed during a network installation operation.

Backing Up, Listing, Verifying, or Restoring from Remote Backup Devices

After Remote Services is configured and remote devices are defined, the only differences in backing up, listing, verifying or restoring data to or from a remote tape drive or file is the initial selection of the device itself. When any backup option is selected from the SMIT menus, a list of available backup devices or directories is displayed.

After a remote server is configured, any device or directories on the server, for which the client has been granted access, are listed as well. The only difference is that the hostname of the server replaces the prefix "Tape," "VirDev," or "Dir" (indicating a tape device, virtual device, and directory respectively).

The SMIT options **List Backup Contents**, **Verify a Backup**, or **Restore Data from a Backup** display a list of devices and a list of available *disk image files* (backups to directory) for all directories on the server the client has access to.

When a server device or directory is selected, the server hostname is transferred to the **Hostname of server** field on the options screen. Then, SMIT includes The hostname of the server in the command to execute.

When executing any SysBack command from the command line, you need to add the "**-h hostname**" flag and parameter to the command to reference a remote, rather than local, device, file or directory.

Configure Remote Services

Before any machine can back up to a remote host, both the client and tape server machines must have Remote Services configured. When selecting this menu option, you are prompted to continue. Press Enter to continue configuring Remote Services.

To configure Remote Services:

1. On the Remote Services menu, select either **Server Options** or **Client Options**, depending on which you are configuring.
2. Select **Configure Remote Services**.
3. When you are asked if you want to continue, press Enter.

You must perform the above steps for each system that you want to use Remote Services. These steps are required before you can select any of the following options.

Adding or Changing Client Host Access to This Server

Before any client host can perform a backup to a remote server, the server must first enable permission to the client host and to the specific users on the client perform the backup operations. Providing access to client hosts does not automatically provide a backup option to the client. After providing access from

the server, you must then use the option **Add or Change List of Remote Backup Servers** on the client to provide a remote backup option in SMIT.

If you want to provide access to the server for all hosts on the network, you can define a single record that applies to all hosts. When doing so, you can exclude or deny access to specific hosts. You do this by providing a permission record for a host called *all*. You might not want certain hosts to have access to all devices and backup directories, so you can deny specific hosts access or change the device or directory list that specific hosts are allowed to use. The devices and directories specified when using this option determine the list of backup options that users on the client host receives when performing backups using SMIT and those devices or directories that other SysBack commands, executed at the command line, are permitted to read or write to.

To add or change client host access to the server:

1. From the Server Options menu, select **Add or Change Host Access to this Server**.

Note: From the command line, use the fastpath `smit sb_cfgremaccess`.

2. Enter the host name for the client system. This can be the name of the client host or *all* to apply the record to all hosts. You can also press F4 to generate a list of hosts already configured to change an existing record. The default entry is *all*.

Note: You can enter either the hostname or a full domain name. If you are operating in a domain network, use the full domain name of the client host. Using only the host name in a domain network allows access to any host on the network with the given host name, even though they might be in different domains.

3. Enter the user name. The default entry is *all*. Press Enter to select this entry, change the entry to another user name, or press F4 to list user records previously configured for the selected host and select a user from the list.

The host name and user name selected are transferred to the following options screen. This example shows the defaults when configuring a permission record for the *root* user on host *venus*:

Add or Change Client Host Access to this Server

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

	[Entry Fields]	
* Hostname of client system	titanic	
If all: Hosts to deny access	<input type="checkbox"/>	+
* User name to allow	all	
If all: Users to deny access	<input type="checkbox"/>	+
Tape or Virtual Devices for backups or "all"	<input type="checkbox"/>	+
Directory path for backup images	<input type="checkbox"/>	+
Directory path for network install images	<input type="checkbox"/>	+

F1=Help
F5=Reset
F9=Shell

F2=Refresh
F6=Command
F10=Exit

F3=Cancel
F7=Edit
Enter=Do

F4=List
F8=Image

Figure 8-4. The defaults When Configuring a Permission Record

4. The fields on the above screen have the following meanings. You can change the fields specified.

Hostname of client system

The hostname entered in the prior screen. You cannot change this field from this screen.

If all: Hosts to deny access

Default=(blank/none). If you selected to add or change the record for "all" hosts, enter a list of hosts, separated by spaces, that are to be explicitly denied access. In other words, all hosts except those specified, will be permitted. When you deny access to a specific host, all users on that host are also denied access.

User name to allow

The user name entered in the prior screen. You cannot change this field from this screen.

If all: Users to deny access

If you selected to add or change the record for "all" users, enter a list of users, separated by spaces, that are to be explicitly denied access. In other words, all users *except* those specified will have access.

If you selected to add or change the record for "all" hosts, the users entered are denied from all hosts. Otherwise, the users entered are denied only from the selected host.

Tape or Virtual Devices for backups or "all"

Default=(blank/none). If the specified user is allowed to back up to a tape drive or virtual device, enter the device name or name, separated by spaces. Press F4 to list the available tape and virtual devices on the system and select one or more devices from the list using F7.

Only the devices entered here are displayed on the SMIT menus when the selected host and user performs a backup to this server.

Directory path for backup images

Default=(blank/none). If you want to allow the specified user to

perform backups to *disk image files*, enter the directory or directories, separated by spaces, that the user can back up to. Press F4 to display a list of backup image directories already selected, or the default directory of **/usr/lpp/sysback/bf/local/username**. Highlight each entry you want to save and press F7. Press Enter to continue.

When performing any SysBack backup, you provided a directory backup option for each directory specified. The actual file created in the directory is named according to the information in Chapter 2, "SMIT Overview", on page 2-1.

Directory path for network install images

Default=(blank/none). This field applies only to the "root" user, because only the root user can create a system backup. Enter information in this field only when configuring the "root" user or "all" users if root is not specifically defined.

Enter each directory for which you want to save installation images, each separated by space. Press the F4 key to display a list of installation image directories already selected, or the default directory of **/usr/lpp/sysback/images/local**. Highlight each entry you want to save and press F7. Press Enter to continue.

When performing the option to **Backup the System**, you are provided a directory backup option for each directory specified. Also, when this or other systems attempt to perform a network installation, all backup images in the specified directories that the client system has permission to read are displayed as network install options.

5. Press Enter to complete this process. Repeat the above steps for each host and user.

Listing Client Access

The **List Client Access** option displays a list of all host and user permission records. The list includes hosts permitted and denied and users permitted and denied for each host. The devices or directories that each host and user are permitted to access are also displayed.

To list the client host access, select **List Client Access** from the Server Options menu. From a command line, you can list host access by typing `smit sb_lsmaccess`.

The list is displayed with no further prompts.

Removing Client Access

Use the **Remove Client Access** option to remove permission records defined in the **Add or Change Client Host Access to this Server** option.

Removing a specific host's permission records does not automatically deny that host access if there is also a permission record defined for "all" hosts. Likewise, if you remove a record containing a list of users to allow, those users are not necessarily denied access if there is also another record for "all" users. If a record exists for "all" hosts and you want to deny access to a specific host, you must remove the host permission record, if any, and then add that host name to the list of hosts to deny using the **Add or Change Client Host Access to this Server** option.

To remove a client permission record:

1. From the Server Options menu, select **Remove Client Access**.

Note: From a command line, type `smit sb_ucfgremaccess`.

A list of hosts with permission records currently defined is displayed.

2. Select a host from the list. If a record exists for “all” hosts, an option for “all” is also shown. If you select to remove the record for “all” hosts, all hosts except those with permission records explicitly defined for them are denied access.
3. After selecting the client host name, a list of users with records defined for that host is displayed. Select a user name, or “all” from the list to remove the selected record.
4. Confirm your choice when asked to do so. This removes the selected permission record from the file with no further prompts.

Adding or Changing the List of Remote Backup Servers

After a backup server has enabled access to a client host using the option **Add or Change Client Host Access to this Server**, the client must identify the servers for which backup options are to be displayed. Only backup options for backup servers defined using this option are displayed when selecting to perform a backup, list, verify or restore operation from SMIT.

To add a remote backup server on the client host:

1. From the Client Options menu, select **Add or Change List of Remote Backup Servers**.

Note: From the command line, type `smit sb_cfgremserver`.

2. The following screen is displayed:

Add or Change list of Remote Backup Servers

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

	[Entry Fields]	
* Hostname of server	[kong]	+
Show disk image file backup/restore options?	no	+

F1=Help

F2=Refresh

F3=Cancel

F4=List

F5=Reset

F6=Command

F7=Edit

F8=Image

F9=Shell

F10=Exit

Enter=Do

Figure 8-5. The Add or Change List of Remote Backup Servers Menu

You can change the following fields on this screen:

Hostname of server

Default=(none/blank). Enter the name of the server to be provided a backup option or press F4 to list the servers previously added and select a server from the list. You can use either the full domain name or just the hostname, as long as the hostname can be resolved by itself.

Show disk image file backup/restore options?

Default=no. With this value set to “no”, no disk image file backup options are displayed for this server. Set this field to “yes” to display disk file options on the server, but the server must have defined one or more directories that are accessible by this client. You are provided a directory backup option for each directory defined on the server.

Even though the server has a directory defined for this host, you might not want to present a backup option. In this case, set this field to “no” and no options are displayed.

3. Press Enter to define this server. You receive an appropriate error message if the server has not yet provided access to this client. When the server is defined, all future backup, list, verify and restore options will provide one or more selections for this server, depending on the number of devices or directories defined for this client.

Listing Remote Backup Servers

This option displays a list of all servers currently defined to this client. This list includes devices and directories accessible to this client, as defined on the server. To list the remote servers and accessible devices and directories, select **List Remote Backup Servers** from the Client Options menu or type `smit sb_lsremserver` at a command line.

The list is displayed with no further prompts.

Changing Remote Access Checking

When doing a backup/restore/verify/recreate using the SMIT interface, and a tape server is down or the network is down, it will cause the SMIT menus to hang or appear to hang waiting on a time out to occur. This feature would disable the remote access checking performed, allowing you to create local backups, or backups to a different remote server, without having SMIT hang. Once disabled, this server remains disabled until you enable it again. However, it does not require that you remove the backup server and it's associated attributes as was previously required to resolve this problem. By default, all backup servers configured by SysBack **Remote Services** are enabled and remain enabled until you specifically disable them.

From the Client Options menu, select **Change Remote Access Checking**.

Note: From the command line, type `smit sb_disableremserver`.

The following screen is displayed:

```
Change Remote Access Checking

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

* Hostname of server (or all)      [Entry Fields]
    Enable/Disable Remote Access  [kong]          +
    Checking                      Enable             +

F1=Help      F2=Refresh   F3=Cancel   F4=List
F5=Reset     F6=Command   F7=Edit     F8=Image
F9=Shell     F10=Exit     Enter=Do
```

Figure 8-6. The Change Remote Access Checking Menu

You can change the following fields on this screen:

Hostname of server (or all)

Enter the name of the server to be enabled or disabled press F4 to list the servers previously configured as remote backup servers and select a server

from the list. You can use either the full domain name or just the hostname, as long as the hostname can be resolved by itself. You may also specify the word ALL to indicate that you would like this action to be performed against all previously defined backup servers.

Enable/Disable Remote Access Checking

Specify to enable or disable the hostname of the system referenced by the **Hostname of server (or all)** field.

Removing a Remote Backup Server

Use the **Remove a Remote Backup Server** option to remove servers defined using the **Add or Change List of Remote Backup Servers** option.

Removing a server from this list does not deny future access to this client, but only prevents remote backup options for this server from appearing on the SMIT menus when you select backup, list, verify, or restore options.

To remove a server from the client:

1. From the Client Options menu, select **Remove a Remote Backup Server**.

Note: From the command line, type `smit sb_ucfgremserver`.

2. Select a server from the list of server hostnames currently defined.
3. Confirm your choice when asked to do so. This removes the selected server from the list.

Remote Commands Access for use with Pull Backups

The **Remote Command Access Options** are used to configure a backup client. This enables a server to remotely initiate a backups (also called a “pull backup.”

For example, the server contacts the client to start the backup. In response, the client initiates the backup and sends data to the server. The server is actually “pulling” the backup operation from the client.

Using pull backups lets you initiate and control backup operations from a single location. You may also automate this backup management using the SysBack Scheduling and Scripting functions described in Chapter 20, “Scheduled Backups and Scripts”, on page 20-1.

Pull backups require Remote Services Configuration and Remote Command Access Configuration. The Remote Services Configuration sends data across the network to the backup server. The Remote Command Access allows the server to initiate the pull backup.

The server that initiates the pull backup does not need to be the server where data is sent. For example, you can configure Remote Service between Machine A, the client, and Machine B, the backup server receiving the backup, and configure Remote Command Access between Machine A, the client, and Machine C, the backup initiation server.

To configure Remote Command Access:

1. Select **Remote Command Access**.

Note: From a command line, type `smit sb_acces`.

2. From the Remote Command Access Menu, select **Configure Remote Services**.

Note: From a command line, type `smit sb_cfgremsvs`.

3. Press Enter at the Are you sure? prompt.
4. Select **Add or Change Remote Command Access**.

Note: From a command line, type `smit sb_accessadd`.

5. Type the fully qualified path name to the desired backup command. The SysBack backup commands are located in Appendix A, "Commands", on page A-1. Commands section of this manual, or you may determine the command by pressing F6 when in a backup menu.

Note: All SysBack backup commands are located in `/usr/sbin`.

6. Enter the fully qualified DNS names of the server system, or systems, that will initiate the backup at the "Hostname of Server System(s)." If you are specifying multiple hosts for which to grant access, you should enter them as a space separated list.
7. If the hostname specified is "all," optionally input any host systems to specifically deny command access at the "If all: Host(s) to deny access" prompt.
8. Press Enter to confirm your selections.

Configuring Remote Services in an NIS Environment

When working in an NIS environment, you should always configure Remote Services (which creates the user `sbnet`) on the NIS Master before configuring it on any NIS Slaves. This is because the Master could propagate the updated user and password files to the Slaves in such an order as to nullify the creation of the `sbnet` user on the Slave after the setup of Remote Services is completed. This could be an inconvenience to figure out when the remote backups from the client fail. The correct order to configure Remote Services are:

1. Configure Remote Services on the NIS Master.

Note: For details, refer to section "Configure Remote Services" on page 8-4.

2. Configure Remote Services on NIS Slaves.

Note: For details, refer to section "Configure Remote Services" on page 8-4.

3. Configure SysBack Remote Service to allow SysBack client access

Note: For details, refer to section "Adding or Changing the List of Remote Backup Servers" on page 8-8.

4. Configure SysBack clients with definitions for the desired remote backup servers.

Note: For details, refer to section "Adding or Changing the List of Remote Backup Servers" on page 8-8.

Chapter 9. Exclude Lists

You might want to exclude certain files, directories, filesystems or logical volumes from a backup to reduce the time needed to make the backup and the amount of space on the backup media. If, for instance, you have a directory that contains only temporary files that are recreated each time an application is started, those files might be excluded from the backup to save time and space. Another example might be read-only data files used by an application that never change. In the case of a system failure, it might be easier to reinstall those data files from another more stationary backup than to include the data on a daily backup.

You can exclude a single file, a directory (and all files beneath that directory), a filesystem, or a logical volume from all SysBack backups.

Note: If a directory name is excluded, all files below that directory are also excluded. This includes any files that might be required for the system to operate properly and might parse into different filesystems. Use discretion when excluding directories to prevent creating a system backup that cannot be used as system installation media.

You cannot use the following characters in the exclude list because they have special meaning to some AIX commands:

\$
*
+
?
^

Although some of these characters can be used in a file or directory name in AIX, those files or directories cannot be properly excluded when entered in the exclude list. Only the asterisk (*) character can be used in the exclude list, but this character represents a *wildcard*, allowing groups of files or directories with similar names to be excluded.

The following are examples of using wild cards in the exclude list:

/*test*	All files in the system containing the word "test".
/*old	All files on the system ending with "old".
/home/b*	All files under /home starting with a "b".
/home/t*y	All files under /home starting with "t" and ending with "y".

Note that any entry starting with "/" includes all directories on the system, not just the root (/) directory.

To access the SysBack menus for managing the exclude lists:

1. At a command line, type `smi t`.
2. Select **IBM Tivoli Storage Manager for System Backup and Recovery**.
3. Select **Configuration Options**.
4. Select **Exclude Lists**.

You can also access these menus using the fastpath. To do this, type `smit sb_exclude` at a command line.



Figure 9-1. The Exclude Lists Menu

Adding a File, Directory or Logical Volume to an Exclude List

To add a file, directory or logical volume to the exclude list, thereby excluding this data from all SysBack backups:

1. From the Exclude Lists menu, select **Add a File, Directory, or Logical Volume to Exclude**.

Note: From the command line, type `smit sb_mkexclude`.

The following screen is displayed:

Add a File, Directory, or Logical Volume to Exclude List

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

[Entry Fields]

Exclude List File Name	<input type="text"/>		
Default file is /usr/lpp/sysback/.exclude_list			
File or directory name to add	<input type="text"/>	/	
OR			
Logical Volume name to add	<input type="text"/>	/	

F1=Help
F5=Reset
F9=Shell

F2=Refresh
F6=Command
F10=Exit

F3=Cancel
F7=Edit
Enter=Do

F4=List
F8=Image

Figure 9-2. The Add a File, Directory, or Logical Volume to Exclude List Menu

2. Enter data into one of the following fields:

Exclude List File Name

Specify the fully qualified path and file name to use as the exclude list. If this field is left blank, the excluded entries will be placed in the default exclude list located at: **/usr/lpp/sysback/.exclude_list**.

File or directory name to add

Default=(blank/none). Enter a filename or directory name to add to the exclude list. The file or directory name must begin with a slash (/), but can contain wildcard (*) characters. If you enter a filename, only that file is excluded. If you enter a directory name, all files and directories within the specified directory are excluded.

If you enter a filesystem mount point for the directory, the entire filesystem is excluded from the backup. This will not, however, prevent the filesystem from being recreated from backups without restoring the data.

Logical Volume name to add

Default=(blank/none). Enter the name of a logical volume to exclude from system and volume group backups. If specified, the logical volume data is not included in the backup, but you can recreate the logical volume from the backup without restoring the data. Enter the logical volume name in the form of /dev/lv00.

3. Press Enter to accept the entries. You must repeat the above steps for each file, directory, or logical volume you want to exclude.

If you prefer, you may create your exclude list directly using the editor of your choice. There should only be one exclude entry per line. When entering logical volumes in this manner, they should be listed as @lvname. For example, /dev/lv00 would be entered in the exclude list file as @lv00.

Below are the contents of a sample exclude list file:

```

root@lasher /usr/lpp/sysback>more .exclude_list
@lv00
@sblv
/lasher/data
/home/*
/tmp/*test*

```

Listing Excluded Files or Directories

To list all of the files, directories or logical volumes currently excluded from SysBack backups, select **Display Current Exclude List** from the **Exclude Lists** menu. You will be prompted for an exclude list file name to display. Enter the fully qualified path and file name to the file to display. If no file name is specified, the **/usr/lpp/sysback/.exclude_list** file will be displayed. All of the files, directories or logical volumes currently excluded from SysBack backups are listed for the specified file.

Removing Files or Directories from an Exclude List

To remove individual files, directories or logical volumes previously added to the exclude list:

1. From the **Exclude Lists** menu, select **Remove Entries from Exclude List**.

Note: From the command line, type `smit sb_rmexclude`.

The following screen is displayed:

Remove Entries from an Exclude List

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

[Entry Fields]

Exclude List File Name

Default file is /usr/lpp/sysback/.exclude_list

File or directory name to add

/

OR

Logical Volume name to add

/

F1=Help
F5=Reset
F9=Shell

F2=Refresh
F6=Command
F10=Exit

F3=Cancel
F7=Edit
Enter=Do

F4=List
F8=Image

Figure 9-3. The Remove Entries from Exclude List Menu

2. Enter data into one of the following fields:

Exclude List File Name

Specify the fully qualified path and file name to use as the exclude list. If this field is left blank, the excluded entries will be placed in the default exclude list located at: **/usr/lpp/sysback/.exclude_list**.

File or directory name to remove

Default=blank. Enter the full pathname of a file or directory to remove or press F4 to list all currently excluded files and directories and select from the list.

Logical Volume name to remove

Default=(blank/none). Enter the name of a logical volume to remove from the exclude list or press F4 to display a list of previously excluded logical volumes and select from the list.

3. Press Enter. Any files, directories or logical volumes removed from the exclude list are now included in all future SysBack backups.

Deleting an Exclude List File

To delete an entire exclude list file:

1. From the **Exclude Lists** menu, select **Delete Exclude List File**.

Note: From the command line, type `smit sb_rmexclude_file`.

The following screen is displayed:

Remove Exclude List File

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

Exclude List File Name

[Entry Fields]
[]

F1=Help
F5=Reset
F9=Shell

F2=Refresh
F6=Command
F10=Exit

F3=Cancel
F7=Edit
Enter=Do

F4=List
F8=Image

Figure 9-4. The Remove Entries from Exclude List Menu

2. Enter data into one of the following fields:

Exclude List File Name

Specify the fully qualified path and file name to use as the exclude list. Unlike the other exclude list options, you may not leave this field left blank. You must explicitly specify the default exclude list located at: `/usr/lpp/sysback/.exclude_list` if you would like to remove it.

3. Press Enter.

Chapter 10. Recreating or Restoring from Backups

There are many reasons to restore data from a backup. The data might have been corrupted due to improper user input or application errors, or the data might be inaccessible due to various hardware problems.

If data was inadvertently deleted or corrupted by a user or application, you will probably need to restore the data from the backup. If a hardware failure occurred, you need to perform additional steps before you can restore the data. For instance, if a disk failure occurs that makes a volume group inaccessible, it will probably be necessary to delete and recreate the volume group, recreate the filesystems and logical volumes, and mount the filesystems, before the data can be restored. Any SysBack backup type can be used in this process, but the backup must contain the desired data, as well as the desired system information, to recreate or restore the desired data.

Note: This section does not describe the process for reinstalling the system, only recreating and restoring data onto an already active system. For information on reinstalling the system from a system backup, refer to Chapter 12, “System Installation and Maintenance”, on page 12-1.

Removing Volume Groups, Logical Volumes, and Filesystems

Before any volume group, logical volume, or filesystem can be recreated on an active system, you must remove the old volume group, logical volume, or filesystem. This process is not detailed within this manual because the steps vary too widely depending on the reason for the recreation process. For detailed assistance on any of these activities, contact your preferred AIX Technical Support Organization. The following guidelines might help in deleting the old system information:

- **Volume Group:** To delete a volume group, first refer to the information below on how to make filesystems and logical volumes inactive. Then, use the AIX **varyoffvg** command to make the volume group inactive and the **exportvg** command to remove the volume group information from the system configuration database.
- **Filesystems:** To delete a filesystem, the filesystem must be unmounted, even if the filesystem is currently inaccessible. You can do this with the AIX **umount** command. To use this command, no user can currently be changed to (**cd** command) any directory within the filesystem, and no process on the system can have any file in the filesystem open.

If you are removing the volume group containing this filesystem, the filesystem will be removed when the volume group is exported. However, to remove only a select filesystem, first unmount the filesystem, then use the AIX **rmfs** command to remove it.

- **Logical Volumes:** To delete a logical volume, no process can have the logical volume open. Certain logical volumes used by the system are normally open by system processes, and the steps to make them inactive vary depending on the logical volume type. To list the logical volumes for a volume group, use the `lsvg -l VGname`

command. This command also shows the logical volume type and whether the logical volume is currently opened (active).

The following information should be helpful for making the logical volume inactive based on its type:

jfs	This is the default logical volume. jfs indicates the logical volume is used for a journaled filesystem. If this is the case, refer to the instructions above for Filesystems. Otherwise, an unknown process on the system has the logical volume open.
jfslog	This is a logical volume used by filesystems in the volume group. This logical volume is made inactive automatically when all of the filesystems that reference it are unmounted. View the /etc/filesystems file to see which filesystems reference which jfslog logical volumes.
paging	This logical volume is a paging space. An active paging space cannot be disabled as long as the system is running. Instead, you must deactivate the paging space for the next system boot using the command chps -an LVname . After doing so, the system must be rebooted for the paging space to be inactive.
dump	This logical volume is used for a system crash dump and is referred to as the dump device. You must disable the system dump to make this logical volume inactive. To do so, execute the command sysdumpdev -Pp /dev/sysdumpnull and sysdumpdev -Ps /dev/sysdumpnull .

Any other logical volume types are user-defined and have no specific meaning to the system.

If you are removing the entire volume group containing the logical volumes, the logical volumes are removed along with the volume group information. If, however, you are only removing the logical volumes, use the **rmlv** command to remove the logical volumes once they are inactive.

Recreating Volume Groups, Logical Volumes, and Filesystems

If you experience a hardware failure that requires you to recreate a volume group, logical volume, or filesystem, you can use either the system or volume group backup. A filesystem backup can also be used to recreate filesystems while a logical volume backup can be used to recreate logical volumes. These “containers” must be recreated to provide a place to restore the data.

You can recreate one or more volume groups, logical volumes or filesystems as they are defined on the backup, or you can optionally change the volume group, logical volume or filesystem characteristics, including the disk location, filesystem and logical volume sizes, or any other attribute.

Note: The containers you want to recreate must have information pertaining to them on the backup media. A volume group backup of only the vg00 volume group cannot be used to recreate any other volume group. However, this backup can be used to recreate single logical volumes or filesystems that were contained within volume group vg00. The system backup, however, always contains information about all volume groups, logical volumes, and filesystems, even if not all volume group data was included on the backup.

You do not have to use the backup media to recreate a volume group, logical volume or filesystem on the same system. You can use the media to perform the recreation on another system, thereby copying an environment from one system to another.

Note that this option recreates the volume group, logical volumes, and filesystems, but cannot restore the data. You can use the **Restore Data from a Backup** option to restore data.

To recreate one or more volume groups, logical volumes, or filesystems:

1. At a command line, type `smi t`.
2. From the SMIT menu, select **IBM Tivoli Storage Manager for System Backup and Recovery**.
3. Select **Backup & Recovery Options**.
4. Select **Recreate Volume Groups, Logical Volumes or Filesystems**.

Note: From a command line, type `smi t sb_create`.

5. On the Device Selector screen, highlight the device you want to use and press Enter.
6. If you selected a tape drive or virtual device, enter the backup sequence number. The default value is "1", indicating that you want to use the first backup on the media. If you "stacked" multiple sequential backups on the media, and want to use the information from a different backup, enter the backup number and press Enter.
If you selected a TSM virtual device, select the TSM Backup ID from the list of backups on the next selector screen.
7. If the backup is a system or volume group backup, select the type of backup you are going to recreate. You have two options:
Volume Group (all LVs and filesystems)
Logical Volume and/or Filesystem

Highlight the type of backup you are creating and press Enter.

If the backup is a Filesystem or Logical Volume Backup, the recreate type is assumed to be "Logical Volume and/or Filesystem."

8. Depending on your response to the previous prompt, select from the displayed list either a volume group or logical volume to create. To select a single option, highlight the option and press Enter. To select multiple options, highlight each option and press F7 to select. When you have made all selections, press Enter to continue.
9. One of the following screens is displayed. These screens are examples of the screens that are displayed when you recreate either a single volume group or two logical volumes from a tape device:

Recreate a Volume Group from a Backup

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

Hostname of Server Device or file name TSM backup ID Edit the Volume Group info before proceeding? New Volume Group Name Volume Group(s) to create	<div style="text-align: right; font-size: small; margin-bottom: 5px;">[Entry Fields]</div> hambone /sysback.images/chukra> yes + [] [vg00]
---	--

F1=Help
F2=Refresh
F3=Cancel
F4=List

F5=Reset
F6=Command
F7=Edit
F8=Image

F9=Shell
F10=Exit
Enter=Do

Figure 10-1. Recreating a Single Volume Group

Recreate a Logical Volume or Filesystem from a Backup

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

Hostname of server Device or file name TSM backup ID Edit the Logical Volume info before proceeding? New Volume Group Name Logical Volume(s) to create	<div style="text-align: right; font-size: small; margin-bottom: 5px;">[Entry Fields]</div> hambone /sysback.images/chukra> yes + [] [lv01]
---	--

F1=Help
F2=Refresh
F3=Cancel
F4=List

F5=Reset
F6=Command
F7=Edit
F8=Image

F9=Shell
F10=Exit
Enter=Do

Figure 10-2. Recreating a Two Logical Volumes from a Tape Device

The following is an explanation of each field:

Hostname of Server

The server hostname if a server option was selected on the prior device selector screen. You cannot change this field.

Device or file name

The device or disk image file name previously selected. You cannot change this field on this screen.

TSM Backup ID

This option will only be displayed when the **Device or file name** is a TSM virtual device. The value for this field is propagated from a previous input screen and may not be changed.

Edit the Logical Volume info before proceeding?

Default=yes. This prompt is displayed only when selecting to recreate logical volumes or filesystems. If you want to view or change the logical volume or filesystem information, such as the disk locations, sizes, or other attributes, before recreating the logical volumes and filesystems, keep the default value of "yes." Otherwise, to recreate the logical volumes or filesystems without viewing or changing the information, press Tab to change the value to "no."

Edit the Volume Group info before proceeding?

Default=yes. This prompt is displayed only when selecting to recreate volume groups. If you want to view or change the volume group, logical volume, or filesystem information, such as the disk locations, sizes, or other attributes, before recreating the volume group and its logical volumes and filesystems, keep the default value of "yes." Otherwise, to recreate the volume group, logical volumes or filesystems without viewing or changing the information, press Tab to change the value to "no."

New Volume Group Name

Default=(blank/none). If you are recreating a volume group, you can enter a new volume group name in this field. This is particularly useful if you want to recreate a volume group but the original volume group by the same name still exists on the system. You can not enter a value in this field if you are creating more than one volume group at one time.

Note: Specify the logical volume name in the form of "lvname" and not "/dev/lvname".

If you are recreating one or more logical volumes, entering a value in this field indicates that the logical volumes to be created will be placed in the specified volume group. In this case, the volume group name you enter must be an active volume group on the system.

New Logical Volume Name

Default=(blank/none). If you are recreating a logical volume, you can enter a new logical volume name in this field. This is particularly useful if you want to recreate a logical volume but the original logical volume by the same name still exists on the system. You can not enter a value in this field if you are creating more than one logical volume at one time.

If you are recreating one or more logical volumes, entering a value in this field indicates that the logical volumes to be created will be placed in the specified volume group. In this case, the volume group name you enter must be an active volume group on the system.

Logical Volume(s) to create

This field is displayed only when selecting to recreate logical volumes and filesystems. This field will contain the names of the logical volumes selected on the prior selection screen. You can change the logical volumes to create by adding or removing entries from this list, separating each entry by a space.

Although only the logical volume name is indicated here, if the logical volume contains a filesystem, the filesystem will be recreated.

Note that information regarding the logical volumes to recreate must be contained on the backup media previously selected.

Volume Group(s) to create

This field is displayed only when selecting to recreate volume groups. This field will contain the names of the volume groups selected on the prior selection screen. You can change the volume groups to create by adding or removing entries from this list, separating each entry by a space. Note that information regarding the volume groups to recreate must be contained on the backup media previously selected.

10. When you have made all selections, press Enter to begin.

The media is read to obtain the information on the volume groups, logical volumes or filesystems selected.

If you selected to edit the volume group, logical volume or filesystem information, a screen similar to the following is displayed:

```
+-----+
| Change Volume Group & Logical Volume Information |
+-----+

Select Physical Volumes for Volume Groups
Change Volume Group Attributes
Select Physical Volumes for Logical Volumes
Change Logical Volume Attributes
Change Filesystem Attributes

+-----+
| Select this option to change the physical volumes which are assigned to each |
| volume group. |
+-----+
| Use ARROW or Tab keys to move and ENTER to Select. Press ESC for Main Menu. |
+-----+
```

Figure 10-3. Editing the Volume Group, Logical Volume, or Filesystem Information

The options for volume groups are not displayed when you select to recreate logical volumes. Also, if this is a power backup, the option for changing filesystem information is not displayed. These menus provide options for changing virtually all attributes for volume groups, logical volumes, and filesystems. This process is identical to reinstalling a system from a system backup. In both cases, the detailed steps for changing this information is provided in Chapter 11, “Changing the Volume Group, Logical Volume and Filesystem Attributes”, on page 11-1.

The volume group, logical volume, and filesystems are then checked to ensure that they can be recreated based on the current system resources available. If there are inconsistencies, such as not enough disk space or unassigned physical volumes (disks), the appropriate messages are displayed and you must change the volume group or logical volume information before the process can continue.

If there are no inconsistencies with the new system, you are asked:

Are you sure you wish to create the volume group(s) (y/n)?

or

Are you sure you wish to create the logical volume(s) (y/n)?

Answering “y” to this question recreates the volume groups or logical volumes as specified. When the process has completed, you are asked to press Enter to return to the SMIT screen.

Understanding Incremental Restores

If you created incremental backups, then you must understand the process of restoring data from these backups. Examples of planning and performing incremental backups and their corresponding restoration processes are detailed in “Understanding Incremental Backups” on page 4-1.

An incremental restore requires restoring a volume group or filesystem to the state of its last full (*level 0*) backup, and then reapplying each subsequent incremental backup level until the volume group or filesystem is returned to its current state. Because only a *level 0* backup contains all of the data in either the volume group or filesystem, this backup must be restored before any additional incremental levels can be applied.

Restoring an incremental backup does not only add or change files in a filesystem, but can also *remove* files from a filesystem. If a file was removed from the filesystem between the time a *level 0* and a *level 1* backup was created, the file can be restored during a *level 0* restore, and removed from the system again during a *level 1* restore.

SysBack does not check the order in which the incremental levels are restored. The user must ensure that the incremental backups are restored in the proper order. SysBack requires that the user explicitly indicate that they want to restore an incremental backup. If an attempt is made to restore a volume group or filesystem from an incremental backup without the user indicating this intent, the restore process does not proceed.

Restoring level 0: When a level 0 backup is restored, the filesystems on the system that are to be restored are first cleared of all files. Then, the backup of the filesystems is restored. At this point, the filesystems have been returned to the exact state at which the level 0 backup was made.

Restoring other levels: After the level 0 backup is applied, the subsequent backup level or levels must be applied to return the filesystems to their most recent state. The number of levels to restore differs depending on the design of the incremental backups. The important thing to remember is that the *most recent* of each subsequent level must be applied in the correct order. If, for instance, you performed multiple *level 3* backups, it is only the most recent level 3 that needs to be restored, because the most recent *level 3* backup supersedes all other *level 3* backups.

Before a level (other than 0) is restored, any files that currently exist in the filesystems, but did *not* exist at the time the backup level was created, are removed from the filesystems.

Restoring individual files or directories: You can restore individual files or directories from any incremental backup level. This is not considered an incremental restore, so it is not necessary to restore a level 0 backup first. If you want to restore the most recent copy of a file, it might be necessary to list the files on each backup level, in reverse order, before finding the file. The file is always included on the level 0 backup (if it existed at that time), but later revisions of the file can be included on any subsequent backup level.

Restoring Data from a Backup

Use the **Restore Data from a Backup** option to restore one or more volume groups, filesystems, logical volumes, directories, or regular files from any type of backup created with SysBack.

To restore from a backup:

1. From the Backup & Recovery Options menu, select **Restore Data from a Backup**.

Note: From the command line, type `smit sb_restore`.

2. On the Device Selector screen, highlight the device you want to use and press Enter.
3. If you selected a tape drive or virtual device, enter the backup sequence number. The default value is "1," indicating that you want to restore data from the first backup on the media. If you "stacked" multiple sequential backups on the media, and want to use the information from a different backup, enter the backup number and press Enter.

The backup media is then read to determine the backup type.

If you selected a TSM virtual device, select the **TSM Backup ID** from the list of backups on the next selector screen.

4. Select the type of data to be restored from the list displayed. The possible choices include:
 - Volume Group (all LVs and filesystems)
 - Filesystem
 - All Directories and Files
 - Directory (all files within)
 - Regular File

Only the options that are valid for the type of backup you are restoring from are displayed. Highlight the type of data you want to restore and press Enter.

5. If you selected volume group, logical volume or filesystem, select the data to be restored from the list of volume groups, logical volumes, or filesystem mount points. To select a single option, highlight the option and press Enter. To select multiple options, highlight each option and press F7. When you have made all selections, press Enter to continue.
6. At the "Do you wish to list select files to restore?" prompt, select "yes" for a list of all files contained on the backup media. You can also narrow the list by using a search word or wildcard character. The search word can include the *wildcard* (*) character. SysBack supports the use of BRE (Basic Regular

Expression) wild cards to restore a wildcard match of files. The filenames and the wildcard must be enclosed in double quotation marks (") to avoid expansion by the user's shell.

For example, the search word `"/home/j*"` indicates to restore all directories and files that start with `"/home/j"` such as `/home/john` or `/home/jenn`. Another example is the search word `"ab*d"`, which would display the following filenames:

```
/tmp/abcd
/var/spool/abduct
/home/data/aboyandhisdog
```

SMIT limitations prevent a list of files longer than 32768 lines from being displayed. Therefore, the list, if longer, is truncated to this size. However, in some cases, SMIT can not handle the excessive size and will display an error. If this occurs, simply restore to the "Do you wish to list select files to restore?" prompt and select "no" instead. You may then specify either a file containing the list of files to restore, or explicitly enter the file names desired.

If you want to display a file that contains a list of files to restore, select "no"

7. The following figures show the default options and values that are displayed when you restore a filesystem from a volume group Backup, and regular files from a filesystem backup:

Restore Data from a Backup

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

	[Entry Fields]	
Hostname of server	hambone	
Disk image file	/sysback.images/chukra>	
TSM backup ID		
Restore data type	Filesystem	
Report output type	both	+
Device name for remote volume prompt	[]	
Allow restore of system data?	no	+
Allow restore of incremental backup?	no	+
Recreate VG, LV, or filesystem before restoring?	no	+
Restore non sparse files as non sparse (AIX 5.1 on ly?)	no	+
Destination (if different)	[]	
Exclude List File Name	[]	+ /
File containing a list of data to be restored	[]	
Data to restore (of above type)	[/fixes]	

F1=Help

F5=Reset

F9=Shell

F2=Refresh

F6=Command

F10=Exit

F3=Cancel

F7=Edit

Enter=Do

F4=List

F8=Image

Figure 10-4. Default Values When Restoring a Filesystem from a Volume Group Backup

Restore Data from a Backup			
Type or select values in entry fields. Press Enter AFTER making all desired changes.			
	[Entry Fields]		
Hostname of server	hambone		
Disk image file	/sysback.images/chukra>		
TSM backup ID			
Restore data type	Filesystem		
Report output type	both	+	
Device name for remote volume prompt	[]		
Allow restore of system data?	no	+	
Allow restore of incremental backup?	no	+	
Recreate VG,LV, or filesystem before restoring?	no	+	
Restore non sparse files as non sparse (AIX 5.1 on ly?)	no	+	
Destination (if different)	[]		
Exclude List File Name	[]	+/	
File containing a list of data to be restored	[]		
Data to restore (of above type)	[/fixes]		
F1=Help F2=Refresh F3=Cancel F4=List F5=Reset F6=Command F7=Edit F8=Image F9=Shell F10=Exit Enter=Do			

Figure 10-5. Default Values When Restoring a File from a Filesystem Backup

The following is an explanation of each field:

Hostname of server

The server hostname if a server option was selected on the prior device selector screen. You cannot change this field.

Device name

The device, if a tape drive or virtual device was selected. You cannot change this field from this screen.

Disk image file

The name of the disk image file previously selected. This field is displayed only if a disk image file name was selected. You cannot change this field from this screen.

TSM Backup ID

This option will only be displayed when the **Device or file name** is a TSM virtual device. The value for this field is propagated from a previous input screen and may not be changed.

Restore data type

The type of data to be restored. This field is for information only and cannot be changed.

Report Output type

Default=progress indicator. Keep the default value if you want to display a progress indicator during the backup process, which indicates the approximate total backup time and amount completed. Press Tab to select "file list" to display a list of files as they are being backed up, or Tab once more to show "only errors" that occur during the backup.

Device name for remote volume prompt

Default=(Blank/None). Enter a TTY, LFT or PTS device name to send the volume prompt to a specified device rather than to the current SMIT screen. If you are backing up to a remote host, the device name you specify is attached to the remote host. This field is displayed only when the backup device is a tape drive or virtual device.

Examples of device names are /dev/tty0, /dev/lft0 and /dev/pts/5. You can determine the terminal device name by typing `tty` at the command line on that device.

Allow restore of system data?

If this field is set to “no”, the restore process cannot restore certain directories, logical volumes, or filesystems that might affect the system operation. Examples are the `hd4` (/ filesystem) logical volume, the `/usr` filesystem, or the `/etc/objrepos` directory. Press Tab to change this field to “yes” if you want to allow any system data to be restored, but be aware that this might cause system errors or a complete system failure depending on the inconsistency of the data being restored and the current system configuration.

Allow restore of incremental backup?

Default=no. Change this field to “yes” if you are restoring entire filesystems or volume groups from an incremental backup. The restoration of incremental data can have a different effect than restoring regular backup data. Information on restoring incremental backups is detailed in “Understanding Incremental Restores” on page 10-7.

An error message is displayed and the process terminates if you attempt to restore data from an incremental backup without setting this field to “yes.”

Recreate VG,LV, or filesystem before restoring?

Specify this option to remake volume group, logical volume, and file system structures before restoring the data.

Note: If you would like to edit any of the LVM attributes associated with the volume group, logical volume, or filesystem before recreating them, you may specify the `-e` flag on the `/usr/sbin/sysrestore` command. This functionality is only available from the command line as there is no SMIT menu equivalent function to edit the attributes.

Instead of using the command line to achieve this functionality, you would simply recreate the LVM structures and restore the data as a two step process. The **Recreate Volume Groups, Logical Volumes & Filesystems** menu allows you to edit the LVM attributes before recreating the structures. Please refer to section “Recreating Volume Groups, Logical Volumes, and Filesystems” on page 10-2 for more information.

Restore non sparse files as non sparse (AIX 5.1 on

Specify this option when there data is being restored to an AIX 5.1 system. You do not have to know which files are sparse vs. non-sparse. This option usually only applies to certain database users restoring database files. Previously, only the AIX `tar` command could restore files as non-sparse. However, in AIX 5.1 the `/usr/sbin/restore` command has been modified to handle this as well.

Note: This option only applies to backups being restored to systems running AIX 5.1 or later.

Destination (if different)

Default = blank. If you are restoring data to its original location, leave this field blank. To select an alternate “relative” logical volume or directory for the restored data, select one of the following:

- For a file/directory backup, enter a new directory. If the file to be restored from the media is **/home/tony** and you want to restore the file to **/tmp** directory, the file is restored “relative” to **/tmp**, resulting in the filename **/tmp/home/tony**.
- For a filesystem backup, enter a new directory. The contents of the entire filesystem will move to the new directory. The new filenames will *not* be relative to the previous filesystem mount point. For instance, the **/home/tony** filesystem (containing the file **/home/tony/file1**) can be moved to the **/test** directory; the resulting file is **/test/file1** (the **/home/tony** directory prefix is removed).
- For logical volume backups, enter a new logical volume name. The data is restored to the new logical volume. An “end of file” error occurs when writing the data if the new logical volume is smaller than the original.

Note: You cannot specify a new destination when you select multiple logical volumes, volume groups, or filesystems to restore.

Exclude List File Name

Specify the fully qualified path and file name of the exclude list to be processed in backup services. If you do not specify a path name along with the file name, the file name specified will be checked for in the **/usr/lpp/sysback** directory.

File Containing a List of Data to be Restored

Specify the fully qualified path name to a file that contains the list of files to be restored from this backup image. Use this option when restoring large numbers of files.

Note: The file list structure should be such that there is only one entry per line in the file. For example:

```
/tmp/myjunk  
/home/*  
/home/my file name that has spaces in it  
/home/my file name with special %&* characters in it
```

This is the only way that SysBack can selectively restore files with spaces or special characters in the path or file name when you input them explicitly. However, if you are specifying a top level directory as the data to restore, and its subdirectories or files have special characters or spaces, there is no need to place them in a file for this option. Also, wildcard restores will correctly restore files and directories that contain spaces or special characters in the name.

For example:

```
/myfs/mydirectory/*
```

A wildcard restore specification such as this could restore files and directories like:

```
/myfs/mydirectory/ my file name  
/myfs/mydirectory/my sub d&rectory/ spec#$@l file  
/yourfs/*
```

A wildcard restore specification such as this could restore files and directories like:

```
/yourfs/speci@l name/dir/dir  
/yourfs/dir name/file@ special
```

Data to restore (of above type)

Unless the backup is a file/directory backup and you select to restore all files and directories, this field contains the data to restore as selected on the prior selection screen. This can be a list of volume groups, filesystems, logical volumes, directories or regular files, depending on the type of backup to be restored. For a file/directory backup, leave this field blank if you want to restore all files.

If you are specifying multiple files or directories to restore, they must be input as a space separated list. If you are using wild cards in your data specifications, the entry must be surrounded by double quotes ("").

For example:

```
/tmp  
"/home/cindy_*"  
"/tmp/g.love"
```

SysBack supports three types of BREs (Basic Regular Expressions):

- Zero or more character match *
- Match one or more in a set []
- Match one character within a range in the set [x-y]

8. Press Enter when all fields have been entered correctly. Either a progress indicator or list of files, if selected, is displayed as the data is read from the media and selected data is restored.

Chapter 11. Changing the Volume Group, Logical Volume and Filesystem Attributes

This section describes the process for changing the volume group, logical volume, and filesystem attributes prior to creating (or recreating) a volume group, logical volume, or filesystem. The same instructions apply to the following SysBack processes:

1. Installation of a system from a SysBack system backup
2. Recreation of a volume group from a system or volume group backup
3. Creation of a logical volume or filesystem from a system, volume group, logical volume or filesystem backup

You can recreate a volume group, logical volume, or filesystem from within the SMIT menus or using the **remakevg** command at the command line.

When you recreate a volume group, logical volume, or filesystem, the information is retrieved from the backup media and compared with the current system configuration to determine if the hardware resources are available to recreate the volume group, logical volume or filesystem as defined on the media. If the configuration matches, you can change the attributes. If the configuration does not match, messages indicate the differences, and you must change the volume group or logical volume attributes to fit the new system.

When you select to recreate a volume group, logical volume, or filesystem on an active system or when you select to **Change Volume Group & Logical Volume Information** when installing from a system backup, a screen similar to the following is displayed:

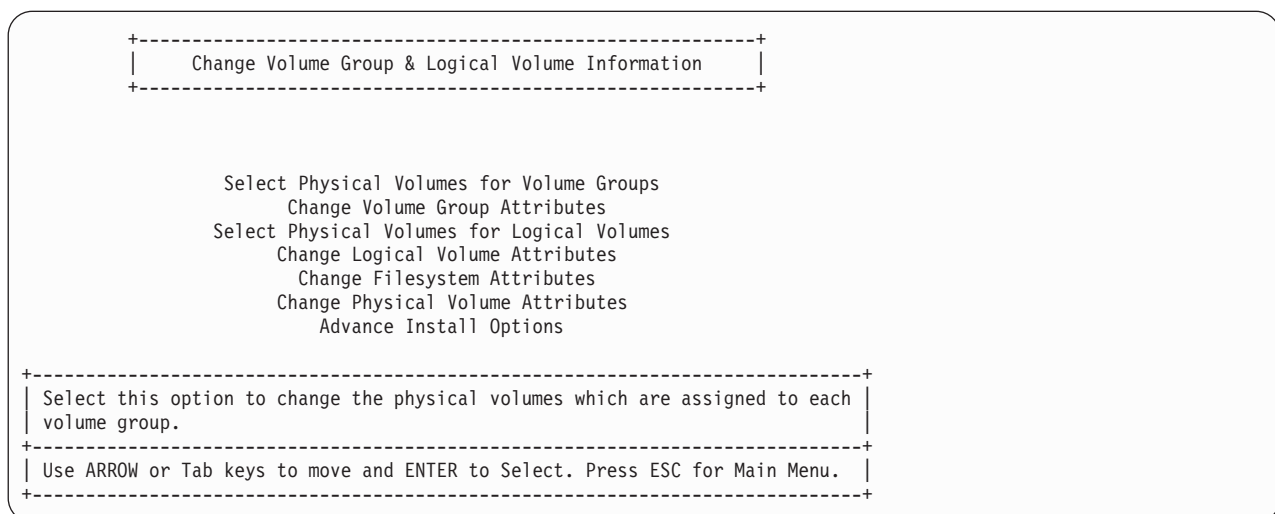


Figure 11-1. The Change Volume Group & Logical Volume Information Menu

Notes:

1. The **Change Filesystem Attributes** option is not displayed if you are installing a system from a power backup.

2. The **Select Physical Volumes for Volume Groups** and **Change Volume Group Attributes** options are not displayed if you have chosen only to recreate specific logical volumes and filesystem from a backup.
3. The **Advance Install Options** menu is only displayed when this menu is invoked by the system installation process.

Press Esc to return to the Main Menu if you are installing a system or to recreate volume groups, logical volumes, or filesystems on an active system.

The following sections describe each option, as shown above, in detail.

Selecting Physical Volumes for Volume Groups

If you select the first option on the menu, a screen similar to the following is displayed:

```

+-----+
|           Select Physical Volumes for Volume Groups           |
+-----+

VG Name      Option  Physical Volume(s)
rootvg       Create  hdisk0
adsmvg       Create  hdisk5 hdisk6 hdisk7
sysbackvg    Create  hdisk1 hdisk2

+-----+
| Select a volume group from the above list.                    |
+-----+
| Use ARROW or Tab keys to move and ENTER to select. Press ESC to cancel. |
+-----+

```

Figure 11-2. The Select Physical Volumes for Volume Groups Menu

Each volume group and a list of physical volumes, if any, currently assigned to the volume group are listed. From this screen, select the volume group for which to change the physical volumes. A screen similar to the following is displayed:


```

+-----+
| Select Physical Volumes for "rootvg" Volume Group |
+-----+

PVname    Location    Volume Group    Description
-----
hdisk0    04-C0-00-4,0    rootvg          16 Bit SCSI Disk Drive
hdisk1    04-02-L          sysbackvg       SSA Logical Disk Drive
hdisk2    04-02-L          sysbackvg       SSA Logical Disk Drive
hdisk3    04-02-L          (free)          SSA Logical Disk Drive
hdisk4    04-02-L          (free)          SSA Logical Disk Drive
hdisk5    04-02-L          adsmvg          SSA Logical Disk Drive
hdisk6    04-02-L          adsmvg          SSA Logical Disk Drive
hdisk7    04-02-L          adsmvg          SSA Logical Disk Drive
hdisk8    04-02-L          (free)          SSA Logical Disk Drive

Megabytes required: 3760    Currently Selected: 4302

+-----+
| Select a PV to add or remove from the "rootvg" volume group. You may NOT |
| select physical volumes currently assigned to a different VG.             |
+-----+
| Use ARROW or Tab keys to move and ENTER to select. Press ESC to cancel.   |
+-----+

```

Figure 11-3. A List of Physical Volumes on a System

This screen contains a list of physical volumes on the system and indicates the volume group to which the physical volume is currently assigned. If a physical volume is not currently assigned to a volume group, (free) will be indicated in the volume group column.

Note:

1. Systems that are using IBM Enterprise Storage Server™, also known as, Shark disks, will be displayed in this list during system installation. However, rebuilding volume groups on to these disks during system installation will not create “vpaths”. It will recreate the volume group to the hdisk name. If you would like your volume group recreated using “vpaths”, specify that the volume group will not be created during system installation and then recreate it with SysBack once the system is up and running.
2. Most EMC® disk drives will be displayed in this list along with their “power disk” names.

Note that the **Megabytes required** field indicates the amount of disk space required to contain the logical volumes defined for this volume group. The **Currently Selected** field contains the amount of disk space selected for the volume group. These fields are updated to reflect any changes to the logical volumes or as physical volumes are added or deleted from volume groups.

You cannot select a physical volume assigned to a volume group, other than the volume group with which you are working. You can add or remove a physical volume from the currently selected volume group by performing one of the following:

- To add a physical volume to the selected volume group, highlight any physical volume marked (free) and press Enter. The name of the selected volume group is added to the **Volume Group** column, and the new megabytes of disk space selected are added to the **Currently Selected** field.
- To remove a physical volume from the selected volume group, highlight a line containing the selected volume group name and press Enter. The volume group

column then indicates (free) and the **Currently Selected** field is updated to reflect the new megabytes of disk space assigned to the volume group.

To move a physical volume assigned to the selected volume group to a different volume group, remove the physical volume from the current volume group, return to the prior menu, then select the new volume group to which you want to add the physical volume.

Press Esc to return to the Change Volume Group & Logical Volume Information menu.

Change Physical Volume Attributes

AIX 5.1 introduced the capability to designate a disk as a hot spare for a given volume group. In order to designate a volume as a hot spare, first assign it to the desired volume group using the **Select Physical Volumes for Volume Groups** menu, then use this menu to designate or change its hot spare status.

The menu will appear similar to the one below:

```

+-----+
| Change Physical Volume Attributes |
+-----+

PVname  Location    Volume Group  Hot   Description
                       Spare
hdisk0   04-C0-00-4,0  rootvg       no    16 Bit SCSI Disk Drive
hdisk1   04-02-L      sysbackvg    no    SSA Logical Disk Drive
hdisk2   04-02-L      sysbackvg    yes   SSA Logical Disk Drive
hdisk5   04-02-L      adsmvg       no    SSA Logical Disk Drive
hdisk6   04-02-L      adsmvg       no    SSA Logical Disk Drive
hdisk7   04-02-L      adsmvg       yes   SSA Logical Disk Drive

Megabytes required: 3760    Currently Selected: 4302

+-----+
| Select a PV to add or remove from the "rootvg" volume group. You may NOT |
| select physical volumes currently assigned to a different VG.             |
+-----+
| Use ARROW or Tab keys to move and ENTER to select. Press ESC to cancel.  |
+-----+

```

Figure 11-4. Change Physical Volume Attributes Menu

To designate a physical volume as a hot spare, highlight the physical volume and press Enter. This will toggle the **Hot Spare** field. Press Enter again to return the **Hot Spare** field to its original value.

Changing Volume Group Attributes

To change the volume group attributes, select **Change Volume Group Attributes** from the menu.

A list of volume groups defined on the media is displayed. Select a volume group and press Enter. A screen similar to the following example is displayed:

```

+-----+
|               Change "adsmvg" Volume Group Attributes               |
+-----+

Attribute                                Value
Install Option                          Create
Auto Varyon at System Startup?          yes
Physical Partition Size (MB)            8
Quorum Checking?                        yes
Copies                                  Not Set
Concurrent-capable?                     no
Auto-concurrent Varyon?                  ***
Big Enabled Volume Group?                no
Factor Size?                             1
Hot Spare?                              no
Logical Track Group Size?                128
Auto-sync?                              no
Filesystem Type?                         Not Set

+-----+
| Type "c" to Create, "i" to Import, or "d" to Delete (ignore).      |
| "Create" will create the volume group and restore data (if on the backup). |
+-----+
| Use UP/DOWN ARROW or Tab to highlight option to change. Press ESC to return. |
+-----+

```

Figure 11-5. The Change Volume Group Attributes Menu

The following is a description of each field:

Install Option

Indicates whether the selected volume group should be created, imported or ignored:

Create Enter "c" to completely recreate the volume group on the specified disks. If installing the system, all logical volume and filesystem data are restored if the data was included on the backup media.

Import

Enter "i" to import the volume group from the physical volumes currently selected for the volume group. If so, the selected physical volumes must currently contain the volume group information.

Delete Enter "d" if you do not want to create the selected volume group. If set to this value, the volume group will be ignored and the physical volumes currently assigned to this volume group can be assigned to another volume group. Any existing data on these volumes will not be destroyed. Therefore, should you decide later to use that data, you may import and vary on the volume group that was previously created on those disks provided that you have not reassigned them to other volume groups.

This option is not available for the rootvg volume group.

Auto Varyon at System Startup?

Press "y" or "n" to indicate whether the volume group should be automatically varied on at system startup. This option cannot be changed for the rootvg volume group.

Physical Partition Size (MB)

Enter a physical partition size in megabytes. Valid options are 2, 4, 8, 16, 32, and 64, 128, 256, 512, and 1024.

Note: The maximum physical partition size varies by level of AIX installed at the time that the backup was created.

If you change the current value, you will receive the following prompt:

Changing the PP size requires the recalculations of all logical volume sizes. Some LVs may increase in size when using a larger PP size.
Are you sure you want to change the PP size? (y/n)

To not change the size, press “n”. Otherwise, press “y”. All logical volume sizes will be recalculated because they are based on the physical partition (logical partition) size of the volume group.

Changing the partition size might require added space to be used by a logical volume. For instance, assume the current volume group has a partition size of 4 MB, and a logical volume within the volume group uses 3 partitions (12 MB). Changing the partition size to 8 MB for the volume group requires that 2 partitions (16 MB) be used for the same logical volume to ensure adequate space for the prior data.

Quorum Checking?

Enter “y” or “n” to indicate whether or not quorum checking should be in effect for this volume group. Quorum checking ensures that there are always a majority of volume group descriptor areas available for this volume group.

Copies

Set this option to globally mirror, or unmirror, all logical volumes in this volume group. By default, this field’s value is Not Set. This means that number of copies of each logical volume will be set exactly as it was on the backup image. Valid options are 1, 2, and 3. If you are increasing the number of copies for the volume group, you must ensure that you have enough disks assigned to the volume group to support the extra copies before beginning the installation.

If you do not have enough disks assigned to the volume group to support the number of copies at the time that the installation is started, SysBack will detect this and prompt you to indicate whether or not that you would like to continue. Indicating a “no” response will return you to the SysBack installation menu so that you can adjust your choices. Indicating a “yes” response will cause SysBack to automatically adjust the number of copies to support the number of disks assigned to the volume group.

Note: If you set this option globally across the volume group, you may override this setting for any individual logical volume to utilized a different number of copies using the **Change Logical Volume Attributes** menu.

Concurrent-capable?

Enter “y” or “n” to indicate whether or not this volume group should be concurrent-capable, allowing the physical volumes in the volume group to be attached to be shared by more than one host.

Auto-concurrent Varyon?

Enter “y” or “n” to indicate whether or not this volume group should be varied on in concurrent mode. This option is not available unless you also selected “y” for the **Concurrent-capable** prompt above.

Big Enabled Volume Group?

Specify “y” to create this volume group as a big enabled volume group which allows greater than 32 disks to be assigned. The maximum number of volumes that may be assigned to this type of volume group is 128. Specify “n” if you do not want the volume group to be created as big enabled.

Factor Size?

Specify a value of 1, 2, or 3 for the volume group’s factor size. The factor size affects the number of physical partitions that may be in the volume group.

Hot Spare?

Specify the hot spare policy for this volume group. You will need to ensure that there is an adequate number of physical volumes assigned to this volume group to support your choice. The valid options are:

- Y** Specify a one to many ratio of disks to hot spare disks in this volume group.
- y** Specify a one to one ratio of disks to hot spare disks in this volume group.
- n** Do not designate hot spares for this volume group.

You must first have assigned the adequate number of physical volumes to this volume group to support your choice using the **Select Physical Volumes for Volume Groups** menu. Also, you must designate the desired assigned disks as hot spares using the **Change Physical Volume Attributes** menu before selecting this option.

Note: This option only applies to backups created on systems running AIX 5.1 or later.

Logical Track Group Size?

Specify the logical track group size in kilobytes to use for disks in this volume group. Valid options are 128, 256, 512, 1024.

Note: This option only applies to backups created on systems running AIX 5.1 or later.

Auto-sync?

Specify “y” or “n” to turn on or off the auto-synchronization of stale partitions in this volume group.

Note: This option only applies to backups created on systems running AIX 5.1 or later.

Filesystem Type?

Set this option to globally set the file system type in this volume group. By default, this field’s value is Not Set. This means that the file system type will be set exactly as it was on the backup image. Valid options are “1” for jfs or “2” for jfs2 file systems.

Note: At the time of this publication’s creation, root filesystems (/ , /usr, /var, /tmp) may only be JFS2 type when created on CHRP hardware using the either 32 bit or 64 bit kernel. This is a limitation of AIX.

If you are changing file systems in the volume group a different type, SysBack will automatically convert or create the appropriate jfs log type to

support each file system type included in the volume group provided that enough disk space is assigned that volume group.

Note: If you set this option globally across the volume group, you may override this setting for any individual file system to utilize a different jfs type using the **Change Filesystem Attributes** menu.

When all selections are complete, press Esc to return to the prior menu.

Note: This option only applies to backups created on systems running AIX 5.1 or later.

Selecting Physical Volumes for Logical Volumes

SysBack, by default, keeps all logical volumes on the same physical volumes as they previously resided, provided that the same physical volumes exist on the current system as those that existed on the original system. If not, the AIX Logical Volume Manager (LVM) automatically determines a default location for each logical volume in the volume group based on its size and other attributes selected.

You can, however, select specific physical volumes where you want to place each logical volume. This is valuable because better I/O performance can be achieved by placing highly-used logical volumes and filesystems on different physical volumes.

When a logical volume is striped across multiple physical volumes, achieving the best I/O performance, you must select the specific physical volumes to use. The number of physical volumes must be a factor of the number of logical partitions (size) of the logical volume.

To select physical volumes where you want to place a logical volume, select **Select Physical Volumes for Logical Volumes**. A screen similar to the following is displayed, showing a list of all logical volumes defined on the backup media:

Select Physical Volumes for a Logical Volume						
LV Name	VG Name	LPs	Copies	StrpSz	NumPVs	MountPoin
hd5	rootvg	1	1	0	1	-
loglv02	adsmvg	1	1	0	1	-
hd8	rootvg	1	1	0	1	-
loglv00	sysbackvg	2	1	0	1	-
hd6	rootvg	40	1	0	1	-
sb1v	rootvg	3	1	0	1	-
hd4	rootvg	4	1	0	1	/
adsm1v	adsmvg	200	1	0	1	/adsmfs
hd1	rootvg	2	1	0	1	/home
lv03	sysbackvg	52	1	0	1	/home/sysback
lv00	sysbackvg	50	1	0	1	/home/sysback/build
lv04	sysbackvg	21	1	0	1	/netscape
MORE..5						
The above logical volumes are for volume groups selected to CREATE. Select a logical volume from the above list.						
Use ARROW or Tab keys to move and ENTER to select. Press ESC to cancel.						

Figure 11-6. A List of All Logical Volumes Defined on the Backup Media

The above screen shows each logical volume and the number of logical partitions, number of copies, stripe size and number of physical volumes currently assigned to the logical volume. Select a logical volume and press Enter. A screen similar to the following is then displayed, showing a list of physical volumes currently assigned to the volume group in which the logical volume exists:

```

+-----+
|          Select PVs for "adsm1v" Logical Volume          |
+-----+

The following are physical volumes in the "adsmvg" volume group:

PVname    Location    Description
==> hdisk5    04-02-L    SSA Logical Disk Drive
hdisk6    04-02-L    SSA Logical Disk Drive
hdisk7    04-02-L    SSA Logical Disk Drive

+-----+
| Select PVs to add to or remove from "adsm1v" logical volume. |
| The "==>" symbol indicates those currently selected.          |
+-----+
| Use ARROW or Tab keys to move, ENTER to select or de-select, ESC to cancel. |
+-----+

```

Figure 11-7. A List of Physical Volumes Assigned to the Volume Group

Select a physical volume and press Enter. The physical volume to use must first be assigned to this volume group using the **Select Physical Volumes for Volume Groups** menu. To deselect a currently selected physical volume, select the volume and press Enter.

Note: Although you can specify specific physical volumes where a logical volume is placed, there is no guarantee that the logical volume will be placed only on those disks unless you create the logical volume using a physical partition map. Verification ensures that adequate space exists in the volume group for all of the logical volumes, but no checks are made to ensure there is adequate space on each disk to satisfy the logical volume selections. If there is not adequate space on the physical volumes when the logical volume is created, it is created using the first available space in the volume group.

When changes are complete, press Esc to return to the previous menu.

Changing Logical Volume Attributes

Use this option to change a wide variety of logical volume characteristics, affecting its size, physical location, and all other attributes.

A screen containing a list of all logical volumes defined on the media is displayed, such as the following example:

```

+-----+
|               Change Logical Volume Attributes               |
+-----+

LV Name      VG Name      Pri    LPs MinLPs Copies MountPoint
hd5          rootvg       03      1     0     1     -
loglv02      adsmvg       04      1     0     1     -
hd8          rootvg       04      1     0     1     -
loglv00      sysbackvg    04      2     0     1     -
hd6          rootvg       10     40     0     1     -
sblv         rootvg       20      3     0     1     -
hd4          rootvg       20      4     2     1     /
adsm1v       adsmvg       20    200    107     1   /adsmfs
hd1          rootvg       20      2     1     1     /home
lv03         sysbackvg    20     52    48     1   /home/sysback
lv00         sysbackvg    20     50    48     1   /home/sysback/build
lv04         sysbackvg    20     21    14     1   /netscape
                                     MORE..5

+-----+
| Select a logical volume from the above list.                |
+-----+
| Use ARROW or Tab keys to move and ENTER to select. Press ESC to cancel. |
+-----+

```

Figure 11-8. A List of All Logical Volumes Defined on the Media

The list of logical volumes includes the creation priority, number of logical partitions (size), minimum recommended partitions, number of copies, and filesystem mount point (if any). If a logical volume had previously been changed so that it would not be created, the line includes the message “*WILL NOT BE CREATED*”.

To change the attributes of a logical volume, select a logical volume and press Enter. A screen such as the following is displayed, indicating the current logical volume attributes:

```

+-----+
|               Change "adsm1v" Logical Volume Attributes       |
+-----+

+-----+
| Original size: 200 LPS (1600 Mb)      (*) VG Space (LPs)    |
| Minimum size: 107 LPS (856 Mb)      Avail Used Free       |
| PVs selected: LV: 1  VG: 3          805  201  604         |
+-----+

Create this LV? *    yes          Inter-policy             m (minimum)
Logical Volume name  adsm1v       Stripe size            0
Volume Group name *  adsmvg       Use PP map?          no
Size (in LPs) *     200           MWC?                  yes
Copies *            1             Write verify?          no
Priority             20            Bad block relocation? yes
Type                jfs           Relocatable?        yes
Intra-policy        c (center)    Maximum PVs         32
Strict              yes           Schedule Policy      p (Parallel)
Mount Point: /adsmfs          Serialize IO          no

+-----+
| Type "n" if you do not want to create this logical volume. If the LV is not |
| created, no data for the LV or its filesystem will be restored.              |
+-----+
| Use UP/DOWN ARROW or Tab to highlight option to change. Press ESC to return. |
+-----+

```

Figure 11-9. The Change Logical Volume Attribute Menu

The box at the upper-left portion of the screen contains information that might assist in making changes to the logical volume size. The **Original size** field

contains the original size of the logical volume. This field does not reflect any changes, so you can always return to this value if you inadvertently change the size. The **Minimum size** indicates the recommended minimum size of a filesystem that is required to contain the filesystem data. The **PVs selected** field contains the number of physical volumes currently assigned to the volume group for this logical volume and to the logical volume itself.

The box at the upper-right portion of the screen contains **VG Space** information for the volume group to which the logical volume is assigned. This information is updated to reflect any changes that are made to the logical volume affecting its size. Also, if the volume group name is changed, the box is updated to reflect the values for the new volume group.

The following fields can be changed for the logical volume:

Create this LV?

Indicates whether or not this logical volume (and filesystem) will be created. If you enter “n” to not create the logical volume, no other fields can be changed. This logical volume is not created and, if installing a system, the logical volume or filesystem data is not restored from the backup media.

If the field currently contains “no,” enter “y” to create the logical volume, and you can then change any other field.

If you change the value of this field, the **VG Space** information box at the top of the screen is updated to reflect the amount of space used in the volume group containing this logical volume.

Logical Volume name

The name of the selected logical volume. You can change the name of the current logical volume by entering a new logical volume name in this field. You can only enter a logical volume that is not currently defined on the active system or on the backup media.

Volume Group name

The volume group in which the logical volume currently exists. To move the logical volume into a different volume group, enter the new volume group name. The volume group name entered must be currently active or must be another volume group recreated from the backup media.

If the volume group name is changed, the **VG Space** information box at the top of the screen is updated to reflect the new volume group.

If the selected logical volume contains a filesystem, then you must use a *Journalled Filesystem Log (jfslog)* logical volume in the new volume group to mount the filesystem. If the logical volume is moved to a new volume group, the **/etc/filesystems** file is updated automatically and the filesystem is mounted using the first available jfslog logical volume in the new volume group. If there is no jfs log for that file system type in the new volume group, SysBack will automatically create one for you provided that there is enough disk space allocated to your volume group.

Size (in LPs)

The size of the logical volume in logical partitions. The actual disk space required by this logical volume is the number of logical partitions multiplied by the number of copies (indicated in the next field). To change the size of the logical volume, enter a new value.

You cannot change this field if you are installing the system from a power backup.

If the logical volume contains a filesystem, the filesystem is created at the same size as the logical volume.

Entering a size smaller than the **minimum size** displayed at the top of the screen might cause you to run out of filesystem space when restoring the data from the backup media. If you are installing a system, over-reducing the root (/) or /usr filesystems usually results in a system installation failure.

When you change the size, the **VG Space** box at the top of the screen is updated to reflect the new amount of space used in the volume group containing this logical volume.

Copies

The number of copies (mirrors) of the logical volume. A "1" indicates there is only one copy or that the logical volume is not mirrored. Changing the number of copies to greater than one causes the logical volume to be "mirrored" to another disk. *Mirroring* is usually implemented to keep a copy of the logical volume on separate physical volumes to protect data against a hardware failure.

The number of copies cannot be changed if the **Stripe Size** is a value other than 0 unless this backup was created on a system running AIX 5.1 or later.

If the number of copies exceeds the number of physical volumes assigned to the logical volume (or volume group if no physical volumes are specifically assigned to this logical volume), you will be asked "Do you wish to allow more than 1 copy on a single PV? (y/n)". If you answer "y", the new number of copies is accepted. If "n", the new value is ignored.

When you change the number of copies, the **VG Space** box at the top of the screen is updated to reflect the new amount of space used in the volume group containing this logical volume.

Priority

The default priority in which the logical volume will be created. This is especially important if different logical volumes might be contending for the same region of a particular disk. Setting the priority of a logical volume to a lower number gives it a higher priority.

By default, the priority is set for logical volumes based on their types. The logical volumes appear in the logical volume list in the order in which you want them created. To create one logical volume before another logical volume, change the priority to less than the other. The next time the logical volumes are listed, the changed logical volume appears in a different place in the list.

Note that this field is a two-digit value, sorted first by the first character, and then by the second. An entry of "1" is sorted after an entry of "06", so use two digits for all entries.

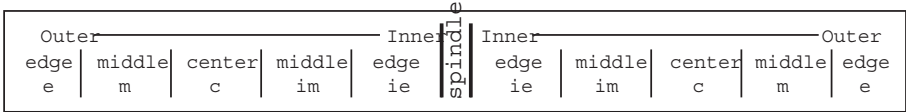
Type

The current logical volume type. The type should not be changed for *paging*, *jfslog*, *dump device*, *boot* logical volumes, and logical volumes assigned to a file system. Although the type "*jfs*" is normally used to indicate filesystem logical volumes, this and other logical volumes, except

those specified above, can be changed to any desired value indicating the type of data contained in the logical volume.

Intra-policy

The current intra-physical volume policy, a policy that determines the region of the physical volumes where the logical volume should be placed. The following diagram indicates the available intra-policies:



This diagram represents a physical volume (or disk drive) and the available regions. In the center of the diagram is the spindle of the disk. To either side of the spindle are the “inner-edge” regions; outside of those are the “inner-middle” regions. You can enter one the following:

- e** edge (or outer-edge)
- m** middle (or outer-middle)
- c** center
- im** inner-middle
- ie** inner-edge

- Strict** Specify the type of strictness policy that you would like for this logical volume. Valid options are:
- y** Specify this option when you would like the logical volume creation to be strict.
 - n** Specify this option when you do not want the logically volume creation to be strict.
 - s** Specify this option when you want the logical volume creation to be super strict.

Mount Point

The directory that is the mount point for logical volumes containing filesystems. If the logical volume does not contain a filesystem a dash (-) is shown in this field and the field cannot be changed.

You cannot change this field if you are installing the system from a power backup.

To change the mount point of the filesystem, enter a new directory here. The directory you specified will be created (if it does not already exist) when the filesystem is created. If installing the system, the data for the filesystem is restored to the new mount point. For example, if the old mount point was **/home/files** and the new mount point is to be **/data/files**, then a file previously called **/home/files/userinfo** is restored as **/data/files/userinfo**.

If changed, the **/etc/filesystems** file is updated to reflect the new mount point for the filesystem so that all future attempts to mount the filesystem will do so to the new mount point.

Inter-policy

The current inter-physical volume policy, which indicates whether or not the logical volume should be spread across multiple disks. This value can have a different affect depending on the following:

- If no physical volumes are selected for the logical volume: a maximum value spreads the logical volume across either all of the disks in the volume group or the value in the **Maximum PVs** field, whichever is less. A *minimum* value uses the first disk in the volume group unless it fills, in which case the next disk in the volume group is used for the remainder.
- If you select physical volumes for this logical volume, a *maximum* value spreads the logical volume across all of the disks selected for the logical volume, not to exceed the value of the **Maximum PVs** field. A *minimum* value uses the first disk in the list should be used unless it fills, in which case the next disk in the list is used.
- If only one disk has been selected for the logical volume or volume group, this policy has no affect.
- If the **Stripe size** is set to any value other than zero (0), this policy has no effect.

Stripe Size

The current stripe size (in K-bytes) or “0” if the logical volume is not striped. Striping a logical volume means that data is inter-dispersed throughout the specific physical volumes in blocks of data indicated by the stripe size. Striping usually benefits random I/O performance, but having a logical volume spread over more than on physical volume causes the entire logical volume to be unreadable if any of the disks containing a part of the logical volume becomes unavailable.

For a logical volume to be striped, you must first assign two or more physical volumes to this logical volume, and the number of **logical partitions** (LPs) must be a multiple of the number of disks selected. You must enter the stripe size in K-bytes (1024 byte blocks). Valid values are 0, 4, 16, 32, 64 or 128. Setting the value to “0” indicates the logical volume will not be striped.

You cannot change this field if you are installing the system from a power backup, if the logical volume is to be created using a partition map (**Use PP map?** field), or if the number of **Copies** is greater than 1.

Use PP map?

Indicates whether or not to preserve physical partition mapping. This value is set to “no” by default, or to “yes” if you selected to preserve physical partition mapping when the backup was created.

Select “y” to retain the exact prior physical partition placement of the logical volume as it was placed on the original system. Creating a logical volume using the partition map is typically performed only if the logical volume was originally created using a partition map. If the logical volume was not originally created using a map, doing so now often retain the partition fragmentation that exists after logical volumes are periodically increased in size. This would usually negatively impact I/O performance to this logical volume.

When you use a map to create a logical volume, the prior physical volumes must still exist and be of the same size. You cannot change the size, number of copies, striping, or physical volumes for a mapped logical volume. Also, the *Intra-policy* and *Inter-policy* are ignored.

Select “n” to not retain the prior physical partition map. In this case, the partitions in the logical volume are created contiguously, resulting, in most cases, in increased I/O performance. The logical volume will, however,

continue to be created in the general location as defined by the physical volume list, Intra-policy and Inter-policy.

MWC?

Indicates whether or not the *mirror-write-consistency* checking is in effect. If so, the volume group status area is updated when writes are performed to a mirrored logical partition. This status is then used, in the case of a disk or system failure, to ensure that all mirrored partitions are identical when the volume group is again varied on. Turning off the MWC increases I/O performance when writing to mirrored logical volumes, but requires you to resynch all mirrors in their entirety in case of an unexpected system halt to ensure all data between the mirrors is consistent.

y Specify this option to turn on active mirror write consistency which ensures data consistency among mirrored copies of a logical volume during normal I/O processing.

P Specify this option to turn on passive mirror write consistency which ensures data consistency among mirrored copies during volume group synchronization after a system interruption.

Note: This option only applies to backups created on systems running AIX 5.1 or later.

n Specify this option when you do not want to enable mirror write consistency for this logical volume.

This field has no effect for single copy (unmirrored) logical volumes.

Write-verify?

Indicates whether a read is performed after every write to ensure the data was written properly. Turning on this attribute decreases the I/O performance when writing to a logical volume but provides higher assurance that data was written properly and is readable. Enter “y” or “n” to change the value.

Bad block relocation?

Indicates whether the software should relocate data in bad blocks when a write error occurs. This action is normally taken by the disk hardware, but the hardware might not have this feature or might not have enough space for the number of blocks to relocate. Turning on this value does not affect I/O performance. To change this value, enter “y” or “n”.

Relocatable?

Indicates whether or not this logical volume can be moved to a new location when a volume group is reorganized using the AIX **reorgvg** or **migratepv** command. If you do not want to enable this logical volume to relocate, enter “y” in this field.

Schedule Policy?

This option changes the scheduling policy when more than one logical partition is written.

p (Parallel)

Specify this option to establish a parallel scheduling policy.

s (Sequential)

Specify this option to establish a sequential scheduling policy.

ps (Parallel Sequential)

Specify this option to establish a parallel write with sequential read

policy. All mirrors are written in parallel but always read from the first mirror if the first mirror is available.

Note: This option only applies to backups created on systems running AIX 5.1 or later.

pr (Parallel Round Robin)

Specify this option to establish a parallel write round robin read. This policy is similar to the parallel policy except an attempt is made to spread the reads to the logical volume more evenly across all mirrors

Note: This option only applies to backups created on systems running AIX 5.1 or later.

Serialize IO?

Use this option to turn on or off serialization of overlapping IOs. If serialization is turned on then overlapping IOs are not allowed on a block range and only a single IO in a block range is processed at any one time. Most applications like file systems and databases do serialization so serialization should be turned off. The default for new logical volumes is off. Valid options are “y” for on and “n” for off.

Note: This option only applies to backups created on systems running AIX 5.2 or later.

Maximum PVs

Specify the maximum number of physical volumes onto which the logical volume can be placed. This value is useful in limiting the number of physical volumes used when the Inter-policy is set to maximum.

The valid values for this option is directly impacted by the **Big Enabled Volume Group** and **Factor Size** options. Please refer to your AIX documentation to determine the maximum allowed PVs based on your configuration choices.

Changing Filesystem Attributes

Selecting this option enables changes to the filesystem attributes for logical volumes to contain filesystem data. This option does not appear when you install from a power backup, because all filesystem data was backed up as raw logical volumes, and changes to the filesystem attributes are overwritten during the restoration of the data.

When you first select the option, the following screen is displayed:

```

+-----+
|               Change Filesystem Attributes               |
+-----+

LV Name      Mount Point      Type
hd4           /                jfs
adsm1v       /adsmfs           jfs
hd1           /home             jfs
lv03          /home/sysback       jfs
lv00          /home/sysback/build    jfs
lv04          /netscape         jfs2
hd3           /tmp              jfs
hd2           /usr              jfs
inst1v       /usr/sys/inst.images jfs
lv01          /usr1             jfs2
hd9var        /var              jfs

+-----+
| Select a filesystem from the above list.                 |
+-----+
| Use ARROW or Tab keys to move and ENTER to select. Press ESC to cancel. |
+-----+

```

Figure 11-10. The Change Filesystem Attributes Menu

Select a filesystem to change and press Enter. A screen similar to the following is displayed, containing the current attributes for the filesystem:

```

+-----+
| Change Filesystem Attributes for "adsm1v" LV             |
+-----+

Attribute      Value
Mount Point    /adsmfs
Fragment Size  4096
Number of Bytes per Inode (NBPI) 4096
Use Data Compression? no
Large File Support? n
Allocation Group (AG) Size 8
Advanced Journal Filesystem? yes
Filesystem Block Size? 1024
Dense Filesystem? no
Use Inline JFS log? yes
Inline Log Size

+-----+
| Type the new top directory where this filesystem is to be mounted. |
+-----+
| Use UP/DOWN ARROW or Tab to highlight option to change. Press ESC to return. |
+-----+

```

Figure 11-11. The Current Attributes for a Filesystem

The following attributes can be changed for the filesystem:

Mount Point

The directory that is the mount point for the filesystem. This field is identical to the **Mount Point** field when changing the logical volume attributes.

To change the mount point of the filesystem, enter a new directory. The directory specified is created (if it does not already exist) when the filesystem is created. If you are installing the system, the data for the filesystem is restored to the new mount point. For example, if the old

mount point was **/home/files** and the new mount point is to be **/data/files**, then a file previously called **/home/files/userinfo** is restored as **/data/files/userinfo**.

If changed, the **/etc/filesystems** file is updated to reflect the new mount point for the filesystem so that all future attempts to mount the filesystem will do so to the new mount point.

Fragment Size

The current filesystem fragment size, or *fragsize*. You can indicate a new fragsize in bytes, and valid values are 512, 1024, 2048, and 4096. If you are using filesystem compression, the fragsize must be set to 2048 or less.

A filesystem containing many small files can benefit from using a small fragsize, as each file requires less space. Larger files with small fragsizes will require more I/O requests and more system processing to read and write larger pieces of data.

Note: If you *increase* the current fragment size value, a filesystem with many small files might require more filesystem space, because each individual file requires more physical disk space. Increasing this value can cause the filesystem to fill when restoring the files. If the filesystem is nearly full, increase the size of the logical volume for this filesystem to provide added space.

Number of Bytes Per Inode (NBPI)

The current NBPI. The NBPI indicates the number of bytes of filesystem space that accounts for each inode in the filesystem inode table.

Enter a new value, which must be 1024, 2048, 4096, 8192, 16384, or 32768. The valid values differ depending on the value in the **Allocation Group (AG) size** field. The valid values are shown at the bottom of the screen.

Note: *Decreasing* the NBPI value might cause a nearly full filesystem to run out of space when restoring a large amount of data, because the filesystem control information uses more space on the disk. *Increasing* the NBPI value uses less space for filesystem control information, but it is possible to run out of filesystem Inodes (assigned to each file) when restoring a large number of files.

Use Data Compression?

Indicates whether or not the data is to be compressed in the filesystem. Enter “y” or “n” to change the current value. Compressing the data requires less disk space, usually between 25% and 50% depending on the type of data. However, each read or write of data requires much more system processing to compress and decompress the data.

Note: If you select not to use compression on a previously compressed filesystem, the data uses more space in the filesystem as it is being restored. Because it is not possible to estimate the amount of added space required, change the logical volume size for this filesystem to at least twice the **Minimum size** indicated at the top of the screen.

Large Files Support?

Indicates whether large files are supported for this filesystem. Only if this field is set to “yes” can you create files larger than 2 gigabytes in size within this filesystem. This field appears only on AIX 4.2 or later systems.

Enabling this support does not affect I/O performance, but the filesystem cannot be remote mounted to another system that does not support this feature. To change the current value, enter “y” or “n”

Allocation Group (AG) Size

Indicates the current allocation group size. The allocation group is a grouping of inodes and disk blocks similar to BSD cylinder groups. This field appears only on AIX 4.2 or later systems.

You can enter a new value in megabytes, which must be 8, 16, 32 or 64. The valid values will differ depending on the value in the **Number of Bytes Per Inode (NBPI)** field. The valid values are shown at the bottom of the screen.

Advanced Journal Filesystem?

Specify “y” or “n” to make this file system a JFS2 file system.

Note: If you do not already have a JFS2 log in this file system’s volume group, and you have not specified to enable an **Inline JFS Log**, then SysBack will automatically create a JFS2 log for you provided that you have enough disk space assigned to support it.

Filesystem Block Size

Use this option to specify the JFS2 block size in bytes. A file system block is the smallest unit of disk storage that can be allocated to a file. Valid options are 512, 1024, 2048, and 4096. This option only applies to JFS2 file systems.

Note: This option only applies to backups created on systems running AIX 5.1 or later.

Dense Filesystem?

This option specifies when files are created with holes JFS2 will allocate disk blocks for those holes and fill them with 0’s. However, this option was mistakenly documented in the AIX 5.1 and 5.2 product manuals. At the time of this publication’s creation, this option is not supported by AIX. This option should always be set to “n” If you mistakenly set this option to “y”, or you have restoring a backup created with an older level of SysBack, the latest SysBack code will automatically correct this value and set it to no.

Use Inline JFS Log?

Specify “y” to this option to place the JFS2 log for this file system in the logical volume along with file system. Valid options are “y” and “n”.

Inline Log Size?

If you have set the **Use Inline JFS Log** to “y”, then use this option to specify the desired size of that log in megabytes. If you do not enter a size and leave the value set to “0”, AIX will automatically determine the size based on its algorithms.

Note: The size may not exceed 10% of the size of the file system.

Advance Install Options

This menu applies to AIX 5.1 and later systems. It will be invoked when you have selected to edit the LBM information when creating an LVM Information file, and during system installation. When you select this menu, below is what will display:

```
+-----+
|               |
| Advance Install Options |
|               |
+-----+

Attribute                                Value
Enable 64 bit Kernel?                    no
Enable JFS2 Filesystems?                  Not Set
Restore non-sparese files as non-spase    no
+-----+
| Type "c" to Create, "i" to Import, or "d" to Delete (ignore). |
| "Create" will create the volume group and restore data (if on the backup). |
+-----+
| Use UP/DOWN ARROW or Tab to highlight option to change. Press ESC to return. |
+-----+
```

Figure 11-12. The Advance Install Options Menu

The following attributes may be changed:

Enable 64 bit Kernel?

Set this option to enable the AIX 64-bit kernel. This assumes that the 64-bit kernel fileset was installed on to the system that created this backup image regardless of whether or not that system was running the 64-bit kernel.

Note: At this time of this publication's creation, this option may only be set for systems that have 64 bit, CHRP hardware. This is a limitation of AIX.

Note: This option only applies to backups created on systems running AIX 5.1 or later.

Enable JFS2 Filesystem?

Set this option to globally set the file system type for all volume groups on this system. By default, this field's value is Not Set. This means that the file system type will be set exactly as it was on the backup image. Valid options are "1" for jfs or "2" for jfs2 file systems.

Note: At this time of this publication's creation, root filesystems (/ , /usr, /var, /tmp) may only be JFS2 type when created on CHRP hardware using the either 32 bit or 64 bit kernel. This is a limitation of AIX.

If you are changing file systems in the volume group a different type, SysBack will automatically convert or create the appropriate jfs log type to support each file system type included in the volume group provided that enough disk space is assigned that volume group.

Note: If you set this option globally across the volume group, you may override this setting for any individual file system to utilize a different jfs type using the **Change Filesystem Attributes menu**.

Note: This option only applies to backups created on systems running AIX 5.1 or later.

If you perform a backup of an AIX 5.1 system, and then change the file system type for rootvg to be different than the type originally backed up, it is highly recommended that you perform a new backup immediately following the system restore. The reason being that you will no longer be able to use this existing backup image in order to boot the system solely for the purpose of importing the rootvg volume group for maintenance. This is because booting a system that is one file system type from a boot image that had a different file system type, will cause needed mounts to fail when attempting to import the root volume group. You will still be able to use this tape to boot and reinstall the system with the settings of your choice, simply not to boot and perform maintains on rootvg.

Restore non-sparse files as non-sparse

Specify this option when there data is being restored to an AIX 5.1 system. You do not have to know which files are sparse vs. non-sparse. This option usually only applies to certain database users restoring database files. Previously, only the AIX tar command could restore files as non-sparse. However, in AIX 5.1 the `/usr/sbin/restore` command has been modified to handle this as well.

Note: This option only applies to backups being restored to systems running AIX 5.1 or later.

Chapter 12. System Installation and Maintenance

A backup created using the **System Backup** option can be used to completely reinstall the original system from which it was made or to install other machines with the same or different hardware configurations. During the installation process, the following functions are provided:

- The volume group, physical volumes, and logical volumes contained on the backup are compared with the current system hardware configuration. If there are inconsistencies, such as missing disks or smaller disks that cannot contain the prior data, you must change the volume group or logical volume information to fit the new system configuration.
- A simple menu interface is provided to change any volume group, logical volume or filesystem size or other attribute. This includes selecting the disks contained in each volume group or the disks where each logical volume will reside. You can also exclude certain volume groups, logical volumes, or filesystems from the installation or move logical volumes and filesystems between volume groups.
- Optionally, individual volume groups, other than rootvg, can be imported from disk (if they currently exist), ignored, or recreated and restored. By default, they are created on the original disks (according to the hardware addresses, if they exist).
- By default, all logical volumes are recreated at their original sizes and on the same disks and disk locations, if available. If original disk locations are not available, the logical volumes are recreated where space permits.
- Logical volumes are, by default, recreated using physical partitions that are contiguous on the disks, unless you specify that the physical partition maps to be preserved when the backup was created. You can also select to change the partition policy for select logical volumes during the installation process. Allowing the partitions to be created contiguously reduces any prior fragmentation that might have existed, thereby increasing the I/O performance to those logical volumes.
- The original device configuration is restored if the same adapters are detected on the new system.

Recovery Installation

One of the options provided on the Utilities menu in the installation menus is to perform a recovery installation. This option enables you to reinstall the operating system from a system backup without affecting other filesystems and logical volumes in the rootvg volume group. This option is not intended for upgrading the operating system level, but recovering from operating system failures. Refer to “Performing Recovery Installation” on page 12-13 for added details.

No-prompt Installation

Installation processes for a client may be configured for a promptless installation. Refer to the **Set Network Install Client Defaults** option in Chapter 13, “Network Boot/Installation Configuration”, on page 13-1 for details on this configuration.

If the client is configured for a no-prompt installation, the **SysBack Installation and Maintenance** menu does not appear as described in the following section, but

the installation proceeds without any input from the user. This occurs if all required default information has been provided and the LVM information on the backup media is compatible with the system to be installed. If, for example, the prior physical volumes are not available or if there is not enough disk space on the client, errors occur, and the installation process defaults to a prompted installation as described in the remainder of this section.

If the installation defaults and backup data are compatible with the client system, the installation proceeds as if you selected the **Install the System with Current Settings** option from the Main Menu.

Note: This feature is not available with system installs from images stored in a TSM server.

Handling Installation Errors

If an error occurs during installation, it occurs in one of the following ways:

1. If the error is a warning message only, the process displays the message and proceeds normally.
2. If the error is recoverable, a message details the error, and you are given the option of either continuing the installation process normally or entering a system maintenance shell. From the maintenance shell (preceded by a `ksh>` prompt), you can manually take whatever steps are needed to recover from the error and then type `exit` to continue the installation.
3. During a no-prompt installation, codes are displayed in the system LED panel indicating both the progress of the installation and if any errors have occurred. If an error that required user intervention occurs, an LED c48 is displayed, the detailed error is displayed on the system console, and the process defaults to a prompted installation. Depending on the point of the error, you are either prompted as described above or placed in the Installation and Maintenance menus.

The system LED displays various codes during a tape or network boot process, as well as various status messages during a no-prompt installation. Refer to Appendix C, “LEDS”, on page C-1 for details on the LED codes.

The SysBack Installation and Maintenance Menu

To display the **SysBack Installation and Maintenance** menu, used to initiate a SysBack system installation, the machine you want to install must first be *booted* from either a SysBack system backup tape, CD or DVD, or a SysBack network boot server.

Note: The Installation and Maintenance menu is not displayed when you perform a no-prompt installation after booting unless an error has occurred in the installation process due to an incompatibility between the information on the backup and the system to be installed.

The instructions for booting the system vary for each boot type and also differ greatly depending on the type of the machine to be booted. Example instructions are provided in Appendix B, “Booting a System for SysBack Installation or Maintenance”, on page B-1 for booting from either tape or network for various hardware architectures. However, you should refer to the documentation that accompanied your particular machine type for detailed instructions regarding system boot procedures.

After you have followed these instructions, the following SysBack Installation and Maintenance menu is displayed:

```

+-----+
| IBM Tivoli Storage Manager for System Backup and Recovery |
+-----+

      +-----+
      | Installation & Maintenance |
      |   M A I N   M E N U   |
      +-----+

Change Installation Device
Change Volume Group & Logical Volume Information
Install the System with Current Settings
Utilities Menu
Reboot the System

+-----+
| Installation Device: Tape Drive [rmt0] |
+-----+
| Use ARROW or Tab keys to move and ENTER to Select. |
+-----+

```

Figure 12-1. The SysBack Installation and Maintenance Menu

The instructions that follow detail the steps for changing the installation options and performing a system installation.

Changing the Installation Device

The default installation device is set to the device the system was booted from and displayed on the main menu. Select the **Change Installation Device** option to change the installation device. After selecting this option, you are presented with a menu similar to the following:

```

+-----+
| Change Installation Device |
+-----+

Device      Description                      Location
==> /dev/rmt0 5.0 GB 8mm Tape Drive                04-C0-00-5,0
/dev/tok0   IBM PCI Tokenring Adapter (14101800 04-05
/dev/ent0   IBM PCI Ethernet Adapter (22100020) 04-B0
/dev/cd0    SCSI Multimedia CD-ROM Drive    04-C0-00-6,0
tsmdev      TSM Virtual Device

Autoloader? No

+-----+
| Select one network device or one or more tape devices. |
| The "==" symbol indicates current choice(s). |
+-----+
| Use ARROW or Tab keys to move, ENTER to select or deselect, ESC when done. |
+-----+

```

Figure 12-2. The Change Installation Device Menu

If you selected a network adapter as the installation device, you can select only one option. However, you can select more than one tape drive as the installation device if you are installing from a parallel backup (created on a parallel virtual device), or if you want to use multiple sequential devices (automatically change to

the next device in the list when prior reaches end of volume). For details on the use of virtual devices, refer to Chapter 21, “Virtual Devices”, on page 21-1.

Important Note: If you are installing from a local parallel virtual device, meaning the backup was striped across multiple physical devices, you must select the same number of devices when performing the installation. You must also insert the tapes in the drives in the order they appear on the Installation Device menu.

Changing the network installation server after a network boot: If you booted from a network boot server but want to install from a device or file on a different network installation server, select the network adapter used to reach the network installation server. You will then be able to change the network settings used to reach the new server.

If you are installing over the network using a TSM virtual device and need to access a different machine as your network install server, you should select the `tsmdev` device entry and not the network adapter used to access that machine. For more information on completing these menus for a TSM network install, please refer “Bare Metal Recovery and System Reinstallation from a TSM Server” on page 15-21 for detailed instructions.

To select a device, highlight the device and press Enter. If the device is a tape, CD, or DVD drive, you can also deselect the device by repeating that action.

If you select a tape device, the **Autoloader** option is displayed. Press either `n` or `y` to change this option to either “no” (default) or “yes.” If you change this option to *yes*, the system will not prompt you to change volumes but will eject the tape cartridge and wait for the autoloader to insert a new cartridge before continuing automatically.

Press Esc to end and return to the Main Menu when you have finished your selection.

Changing the Network Settings

If you selected a network adapter option, the following screen is displayed, based on the network adapter type selected:


```

+-----+
|               Change Network Settings               |
+-----+

Client IP Address      192.168.1.58
Server IP Address      192.168.1.55
Gateway IP Address     192.168.1.55
Subnet Mask            255.255.255.0

Ethernet Interface:
==> Standard Ethernet Interface
    IEEE 802.3 Ethernet Interface
Ethernet Connection Type:
==> BNC: Coax Cable
    DIX: 15-pin D-shell Cable

Network Adapter: ent0 [inactive]
+-----+
| Enter the subnet mask, if any, in the format "255.255.255.255". Leave this |
| field blank if no subnet mask is used.                                   |
+-----+
| Use ARROWS or TAB to move or INS/DEL to edit. Press ESC to return.       |
+-----+

```

Figure 12-3. The Change Network Settings Options for a Network Adapter

If you selected an Ethernet adapter, you are presented with options similar to the following:

```

+-----+
|               Change Network Settings               |
+-----+

Client IP Address      192.168.1.58
Server IP Address      192.168.1.55
Gateway IP Address     192.168.1.55
Subnet Mask            255.255.255.0

Ethernet Interface:
==> Standard Ethernet Interface
    IEEE 802.3 Ethernet Interface
Ethernet Connection Type:
==> BNC: Coax Cable
    DIX: 15-pin D-shell Cable

Network Adapter: ent0 [inactive]
+-----+
| Enter the subnet mask, if any, in the format "255.255.255.255". Leave this |
| field blank if no subnet mask is used.                                   |
+-----+
| Use ARROWS or Tab to move or INS/DEL to edit. Press ESC to return.       |
+-----+

```

Figure 12-4. The Change Network Settings Options for an Ethernet Adapter

If you selected a token ring adapter, you receive options similar to the following:

```

+-----+
|               Change Network Settings               |
+-----+

Client IP Address      192.168.1.58
Server IP Address      192.168.1.55
Gateway IP Address      192.168.1.55
Subnet Mask            255.255.255.0

Token-ring Speed:
    4 Megabits
==> 16 Megabits

Network Adapter: tok0 [inactive]
+-----+
| Enter the IP address by which the server refers to this host in the format |
| "111.222.333.444". You need not include leading zeros.                    |
+-----+
| Use ARROWS or TAB to move or INS/DEL to edit. Press ESC to return.        |
+-----+

```

Figure 12-5. The Change Network Settings Options for a Token Ring Adapter

If you selected an FDDI adapter, you receive options similar to those above, except that the token ring speed option is not displayed. There are no options specific to the FDDI adapter.

If you booted from a network boot server, the addresses and subnet mask used to boot the system are displayed. Otherwise, if the boot media was created on a system previously network-installed using SysBack, the prior network installation settings are displayed.

To change the **client**, **server** or **gateway IP address**, or the **subnet mask**, highlight the line you want to change and enter the new value.

Note: If the client and the network install server are on the same subnet, and the client does not have to pass through a network gateway in order to reach the server, it is recommended that you re-enter the **Server Address** in the **Gateway Address** field. If the client and the network install server are on different subnets, you would enter the network gateway address in the **Gateway Address** field.

To change the **ethernet interface**, **ethernet connection type** or **token ring speed**, highlight the desired selection and press Enter.

When all selections are complete, press Esc to return to the previous menu.

If you are installing over the network using a TSM virtual device and need to access a different machine as your network install server, you should select the `tsmdev` device entry and not the network adapter used to access that machine. For more information on completing these menus for a TSM network install, please refer "Bare Metal Recovery and System Reinstallation from a TSM Server" on page 15-21 for detailed instructions.

Important note: For token ring networks, be certain to select the correct token ring speed. Not doing so could cause disruption on the entire network when the token ring adapter is configured.

Changing Volume Group & Logical Volume Information

The SysBack installation process enables you to fully customize the sizes, locations, and other attributes for volume groups, logical volumes, and filesystems.

If you are installing from a network tape drive, CD, or DVD, or a disk image file, the network installation server is contacted to obtain a list of tape drives, virtual devices, or disk image files available to this client. If any options are available, a screen titled “Select Source for Volume Group Data” is displayed. You must select a single option from which you want the data for the volume groups to be restored.

If you are restoring from a TSM server, you will be prompted to select the **Backup ID** to use for the install rather than a list of devices from which to restore.

After selecting to change the system settings, the system verifies the volume group information from the backup media against the current system configuration. A screen similar to the following is displayed:

```
+-----+
|               Verifying LVM Information ..               |
+-----+
| COMPLETE |
+-----+
|
| The following errors were found in the volume group records:
| -----
| > Physical Volume ID 0016652284a18698 (previously hdisk0 at
|   location 04-C0-00-4,0) does not exist on this system.
| > There are no physical volumes remaining for the rootvg volume
|   group. You must assign at least one physical volume to rootvg before
|   continuing.
|
+-----+
| The above errors must be corrected before the installation may be performed.
|
+-----+
|               Press ENTER to continue.
|
+-----+
```

Figure 12-6. An Example Backup Installation Screen

The above screen provides an example in which a backup is being installed on a different system with physical volumes (disks) that do not match the disk configuration of the original system from which the backup was taken. If there are no inconsistencies, this screen shows no errors and no prompts appear.

After the verification process is complete, the following screen is displayed, providing options for changing volume group, logical volume and filesystem options:

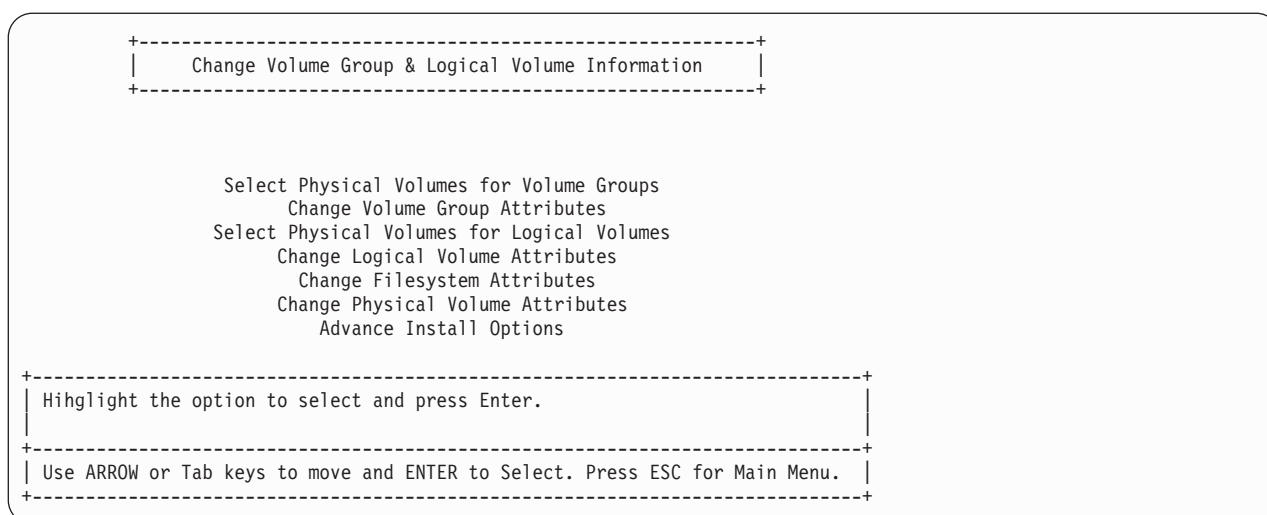


Figure 12-7. The Change Volume Group & Logical Volume Information Menu

The option for changing filesystem options is not displayed if the backup media is a *power backup*. Since the power backup contains only raw logical volumes, no filesystem information can be changed.

The current settings for each volume group are displayed. You can change the settings for a volume group or for the logical volumes within the volume group by selecting the line number corresponding to the volume group name.

The remaining steps required to change the volume group and logical volume information is identical to the process for editing the volume group and logical volume attributes when recreating a volume group or logical volume on a running system. These instructions are provided in Chapter 11, “Changing the Volume Group, Logical Volume and Filesystem Attributes”, on page 11-1.

When you finish your changes, press Esc to return to the Main Menu.

Installing the System with Current Settings

When you have made all selections, such as changing of the installation device or the volume group and logical volume characteristics, you can continue the installation by selecting **Install the System with Current Settings** on the Main Menu.

If you are installing from a *network installation server* or a TSM server and did not previously select to edit the volume group attributes, the server is contacted and a list of available system backup disk image files and installation devices are displayed. You must select a disk image file or device from which the volume group data is restored.

The system again compares the current hardware configuration with the volume group and logical volume attributes from the backup, including any changes you made from the installation menus, to verify that there is adequate space on the system to continue the installation. If not, a message indicating the problem is displayed and you return to the Main Menu.

If no inconsistencies are found in the system configuration, preventing the installation from proceeding, a confirmation screen similar to the following example is displayed:

```

+-----+
|               Install the System               |
+-----+
| Verifying space requirements ..                  |
+-----+
| VG Name      Available MB    Used MB    Free MB  |
|-----|-----|-----|-----|
| rootvg       1996 (249 PPs)   1352 (169 PPs)  644 (80 PPs) |
|-----|-----|-----|-----|
|
|
|
|
|
|
|
|
|
|
|
+-----+
| Continuing the installation at this time will overwrite all disks used by |
| volume groups you chose to create!                                       |
+-----+
| Do you wish to continue the installation? (y/n)                         |
+-----+

```

Figure 12-8. An Installation Confirmation Screen

Press *y* to continue with the installation or *n* to return to the Main Menu.

For systems with system keys, you can turn the system key to the normal position at any time to enable the system to reboot in normal mode without prompting the user at the end of the installation.

The installation process performs the following steps:

1. The *rootvg* volume group is created, as well as all logical volumes and filesystems in the *rootvg* volume group.
2. The *root* (/) and */usr* filesystem data is restored.
3. The user *post-root install* script is executed if it exists. Refer to Appendix D, "Creating Scripts for Customizing the System Backup and Install Process", on page D-1 for details on the postroot installation script.
4. Root volume group post-installation processing occurs. An example of this processing is updating the device configuration with the new system configuration and rebuilding the boot logical volumes.
5. Each additional volume group, and the logical volumes and filesystems, are created.
6. The filesystem and logical volume data are restored for all remaining logical volumes and filesystems for which data is present on the backup media.
7. The user *post-installation* script is executed if it exists. Refer to Appendix D, "Creating Scripts for Customizing the System Backup and Install Process", on page D-1 for details on the post-installation script.
8. If you are installing on a different machine other than the one used to make the original backup, you are asked if SysBack should be removed from the machine unless you have pre-configured this response in the **Utilities** menu. Details for this prompt are described in "Removing IBM Tivoli Storage Manager for System Backup and Recovery from a Non-licensed Machine" on page 12-10.

9. If you are installing on a different machine than the original backup was made from and the original machine was configured on a network, you are asked if you want to remove the network configuration unless you pre configured this response in the **Utilities** menu. Details for this prompt are described in “Removing the Network Configuration” on page 12-11.
10. If a system key exists and is in the *normal* position, the system is rebooted automatically. Otherwise, you are prompted to turn the key to normal position and press Enter to reboot. You then see the following message:

Re-applying device configuration from previous install...

The system will now shutdown and reboot in order to activate the device configuration changes...

The system shuts down and reboots once more. When the installation is complete, the system should look exactly like the original system from which the backup was made, with the exception of any changes that you specified during the installation process. If, however, devices were defined on the original system, and the same physical devices or adapters do not exist on the system on which you are installing on, those devices will not be defined to the new system.

Removing IBM Tivoli Storage Manager for System Backup and Recovery from a Non-licensed Machine

Because SysBack provides the ability to back up one machine and use that backup to install another, you replicate the SysBack programs as well. If you do not own a license of the product for the machine that you are installing, then you must remove SysBack from the system after the installation.

To accommodate this, the installation process will check to see if you have installed on the same system from which the backup was originally created. If so, SysBack is retained. If not, the following message will appear at the end of the installation process, just prior to rebooting:

This system was installed from a backup originating from another machine.
If you do not have a license of IBM Tivoli Storage Manager for System Backup and Recovery for this
Should SysBack be removed from this system? (yes/no) ==>

If SysBack is not licensed on the current machine, type yes to automatically remove SysBack from the newly installed system. Typing no retains SysBack from the original backup.

If at a later time you want to remove SysBack from the system, you can do so by logging in as “root” and typing the following at the command line:

```
/usr/lpp/sysback/rmsysback
```

This removes all SysBack programs and installation history from the system.

However, if you are using the IBM Tivoli Storage Manager for System Backup and Recovery version of SysBack, the product is removed through the standard AIX software removal process using the “installp” command.

If you are installing a backup on an LPAR capable machine, that was made from another partition in that same machine, this prompt will not occur. However, if

you would like to remove the product from the new partition, you may configure SysBack to do so using the Utilities menu option described in “Utilities Menu” of this chapter.

Removing the Network Configuration

If you are installing the machine from a backup that was made on a different machine and the original machine was configured on a network, the current network settings, including the hostname, IP address and netmask are restored as well. You can remove the network configuration from this newly installed system during the installation process is desired.

The reason for removing the network configuration at this time is to avoid conflicts with another machine with the same settings that might be currently active on the network. Allowing a machine installation with a network definition that conflicts with another active machine might cause severe network problems.

To remove the network configuration at this time, you will need to enter the correct settings after the installation is complete using the standard SMIT process for configuring TCP/IP.

To accommodate this, the installation process will check to see if you have installed on the same system from which the backup was originally created. If so, SysBack is retained. If not, the following message will appear at the end of the installation process, just prior to rebooting:

This system was installed from a backup originating from another machine.
If you would like to remove the network settings contained in the backup for this machine, you s
Would you like to remove network settings from this system? (yes/no) ==>

If you would like to have SysBack remove the network settings for this machine, type yes to automatically remove them. Typing no retains the network settings from the original backup.

If you are installing a backup on an LPAR capable machine, that was made from another partition in that same machine, this prompt will not occur. However, if you would like to remove the network settings from the new partition, you may configure SysBack to do so using the Utilities menu option described in “Utilities Menu” on page 12-11 of this chapter.

Utilities Menu

The **Utilities Menu** option provides the following options:

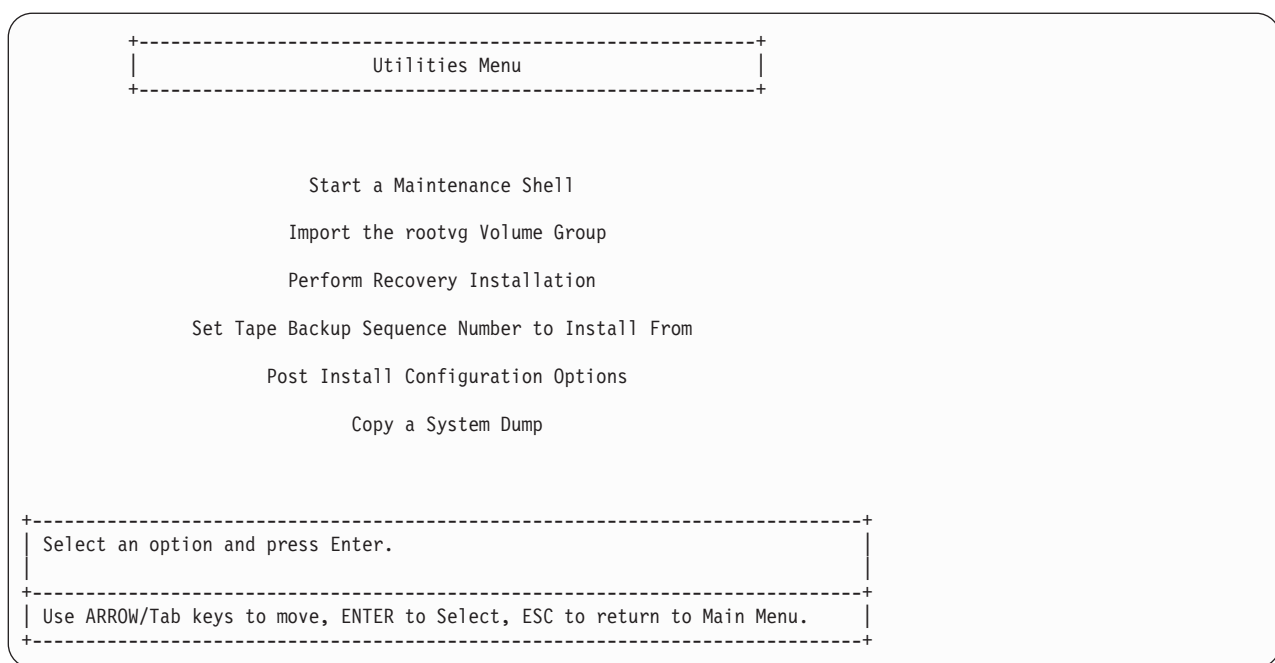


Figure 12-9. The Utilities Menu

Each of the options provided on this menu are described below.

Starting a Maintenance Shell

This option places you at a shell prompt and enables you to perform system maintenance tasks. The following message is displayed:

```

You have entered a maintenance shell. When finished, type "exit" to
return to the Main Menu...

ksh> _

```

The maintenance shell is provided for the experienced user, typically to perform system recovery without reinstalling the system. Details for those tasks are beyond the scope of SysBack function and are not provided here.

You can return to the Main Menu by typing exit.

Importing the rootvg Volume Group

This option provides the ability to gain access to the operating system data, provided that a *rootvg volume group* already exists on one or more disks on the system.

After selecting this option, you are provided a list of physical volumes that exist on the system and a list of logical volumes that reside on those disks. You must select only one physical volume containing the rootvg volume group to import. Some systems might have more than one rootvg volume group.

It is important that you select a physical volume containing a rootvg volume group. SysBack cannot determine which disks have a rootvg volume group because the volume group information does not include the name of the volume group. However, you should be able to determine the rootvg volume group by looking at the list of logical volumes contained in the volume group.

After you have selected a rootvg volume group to import, you are asked:

Mount filesystems after importing?

Type *y* or *n* to indicate whether or not the filesystems in the rootvg volume group should be mounted after the volume group is imported. When performing some maintenance tasks, such as checking and repairing the root (/) or /usr filesystem, you would not want to mount the filesystems at this time.

After you make your selection, the rootvg volume group is imported, the root (/) and /usr filesystems are checked and repaired if necessary, and then all filesystems are optionally mounted. If you chose to mount the filesystems, you are then asked:

Do you want to rebuild the boot logical volume now?

Type *y* or *n* to indicate if the boot logical volume should be rebuilt using the AIX **bosboot** command. Doing so can recover from many operating system failures but causes no harm.

You are then placed in a maintenance shell (preceded by the “ksh>” prompt. You can perform operating system commands from this prompt. When ready, use normal operating system procedures for rebooting the system.

Performing Recovery Installation

A recovery installation will restore only the operating system on the client by performing the following steps:

1. Import a *rootvg* volume group.
2. Check, repair if needed, and mount the root (/) and /usr filesystems.
3. Restore the root (/) and /usr filesystem data from the backup media.
4. Rebuild the boot logical volume.
5. Reboot the system.

This process is *not* intended for updating the operating system on the client. It is used to restore the primary operating system filesystems from the client’s backup. It might be possible to restore the data from a backup taken from another machine, but note that, because only the root (/) and /usr filesystem data is being restored, there might be incompatibility with other data in the rootvg volume group.

After you select this option, the LVM information is read from the backup media and you are provided a list of physical volumes that exist on the system and a list of logical volumes that reside on those disks. You must select only one physical volume containing the root (/) and /usr filesystems to be restored. Some systems might have more than one rootvg volume group.

It is important that you select a physical volume containing a rootvg volume group. SysBack cannot determine which disks have a rootvg because the volume group information does not include the name of the volume group. However, you should be able to determine the rootvg volume group by looking at the list of logical volumes contained in the volume group.

After you select the rootvg volume group to use, the volume group will be imported. You are then asked:

Do you wish to view/change the logical volume or filesystem info?

Type y or n to indicate if you want to view or change the attributes for the root (/) and /usr filesystems or logical volumes. This includes such attributes as the size and disk location of these logical volumes. This provides, for example, an effective tool for reducing the size of an over-expanded /usr filesystem without having to reinstall the entire operating system. Refer to Chapter 11, “Changing the Volume Group, Logical Volume and Filesystem Attributes”, on page 11-1 for additional details.

You have one final prompt to determine if you want to continue the installation process. Then the recovery installation begins. If the operating system was restored from a backup taken from a different machine than the client, you might also be asked whether or not to remove the SysBack product and the network configuration. Refer to “Installing the System with Current Settings” on page 12-8 for additional information on these prompts. Upon completion, the system reboots automatically.

Setting Tape Backup Sequence Number to Install From

If you are installing from tape media, and you have “stacked” system backups onto the tapes, you might want to install from a system backup other than the first backup on the tape. If so, you must select the correct backup sequence number using this option. Although no action is performed on the media at this time, changing the backup sequence number to anything other than “1” (the first system backup on the media) causes the media to be forwarded to the correct system backup before any additional installation processing occurs.

After selecting this option, you are prompted for the backup sequence number to use. You must enter “1” for the first backup on the media, or any number up to the number of system backups performed to the media. After making your selection, you return to the Utilities menu.

Post Install Configuration Options

The Post Install Configuration Options enables you set certain common user prompts that display during an installation. Setting the response to these prompts before installation is a convenient way to minimize the intervention required during normal installation processing - especially when cloning a backup image from one machine to another.

From the installation main menu, select **Post Install Configuration Options** to display the following menu:

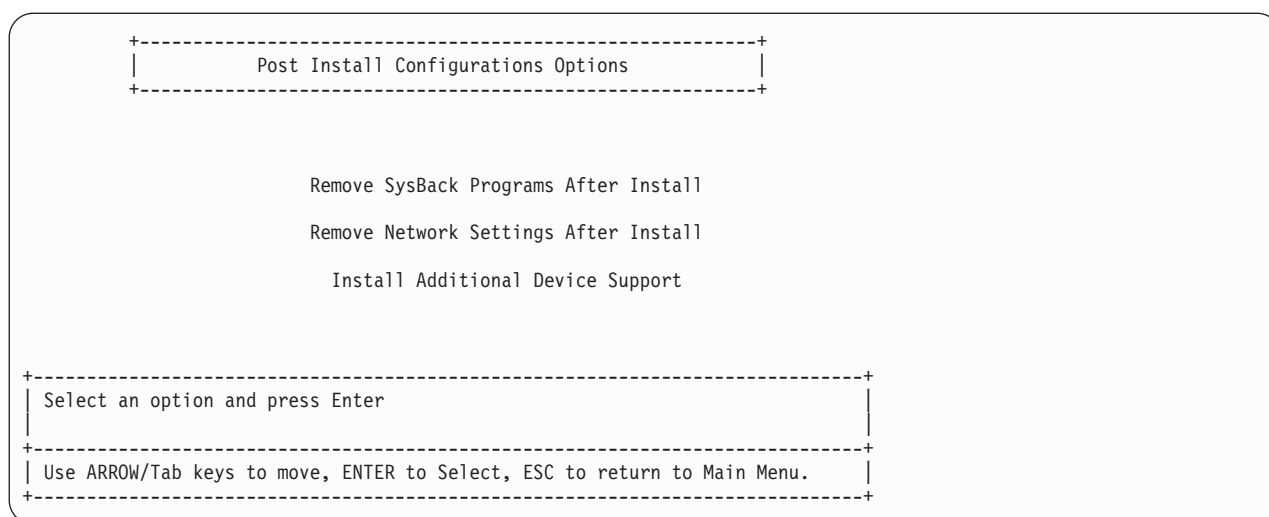


Figure 12-10. The Post Install Configuration Options Menu

Remove SysBack Programs After Install: Selecting the **Remove SysBack Programs After Install** option displays the following menu:

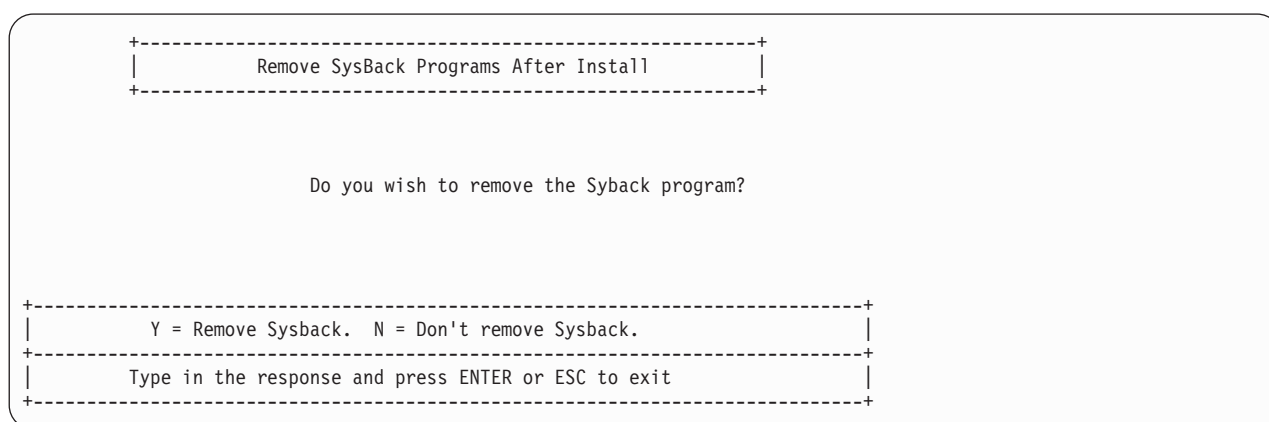


Figure 12-11. The Remove SysBack Programs After Install Menu

This yes or no option indicates whether to remove the Sysback program from the system after an installation. This is useful when the user has not purchased a license for the client that will be installed. The default is no.

If you did not set this option prior to installation, you will be prompted for a response as described in “Removing IBM Tivoli Storage Manager for System Backup and Recovery from a Non-licensed Machine” on page 12-10 of this chapter.

This option can also be set prior to installation using the Set Network Install Client Defaults Menu described in “Setting the Network Install Client Defaults” on page 13-5, “Changing SysBack Tape Boot Defaults” on page 16-9, and “Changing SysBack CD/DVD Boot Defaults” on page 16-12.

Once you have made your selection, press ESC to return to the previous menu.

Remove Network Settings After Install: Selecting the **Remove Network Settings After Install** option displays the following menu:

```

+-----+
| Remove Network Settings After Install |
+-----+

Do you wish to remove the network settings?

+-----+
| Y = Remove network settings. N = Don't remove network settings. |
+-----+
| Type in the response and press ENTER or ESC to exit |
+-----+

```

Figure 12-12. The Remove Network Settings After Install Menu

This yes or no option indicates whether to remove network specific information required to configure the host to the network. This option is useful when the machine installed was cloned from the backup image of a machine that is still present on the network. The default is no.

This option can also be set prior to installation using the Set Network Install Client Defaults Menu described in “Setting the Network Install Client Defaults” on page 13-5 in Chapter 13, or “Changing SysBack Tape Boot Defaults” on page 16-9 in Chapter 15.

Once you have made your selection, press ESC to return to the previous menu.

Install Additional Device Support: Selecting the **Install Additional Device Support** option displays the following menu:

```

+-----+
| Install Additional Device Support |
+-----+

Install Device
Device Support To Install Minimum

+-----+
| This option can be a locally attached install device like a tape drive |
| (/dev/rmt#) and cdrom (/dev/cd#) or an NFS mounted LPP Source Directory |
+-----+
| Use ARROW/TAB keys to move, ENTER to Select, ESC to return to Main Menu. |
+-----+

```

Figure 12-13. The Remove SysBack Programs After Install Menu

Install Device

This option lets you specify a CDROM device name, a tape device name, or a NIM **LPPSOURCE** directory name. The NIM **LPPSOURCE** directory name provides additional device support to install during installation. This device support, if available in the specified location, will be installed in circumstances where the needed device support for this machine is contained in the boot image, not the backup image to be installed.

If this is a NIM Resource Network Boot, SysBack will automatically pull device support from the NIM **LPPSOURCE** specified when the Network

Boot client was added regardless of whether this option is edited. For more information on configuring a NIM Resource Network Boot, see Chapter 13, “Network Boot/Installation Configuration”, on page 13-1.

Device Support to Install

This option tells SysBack how much to install of what is contained in the media in the location specified by the **Install Device** option. The two options are:

Minimum

Selecting this option will install only those device support filesets identified by AIX when the system was booted. This information is obtained from the file `/tmp/devices.pkgs` which is created by AIX when the system was booted. This file is not always 100% accurate regarding what device support is needed as some devices return invalid installp package names rather than individual filesets. In most cases, however, this is a reliable alternative to pre-installing all device support filesets on to a system prior to creating the backup image.

All Selecting this option tells SysBack to perform an install command against every item contained on the media in the specified location. This may include device support filesets or any other software that is located on the media.

Once you have made your selection, press ESC to return to the previous menu.

Copying a System Dump

A system dump is recorded when a hardware failure renders the system inoperable or when the system user initiates a dump manually. The system dump is stored in a logical volume designated as a *dump device*. The system always stops after a system dump is recorded.

This option copies the information from the dump device to a tape for later analysis by experienced AIX system support personnel.

When you first select this option, information regarding the last recorded system dump is displayed on the screen, such as the following:

```
Date:      Tue Nov 11 18:58:55 1997
Dump device:  /dev/hd6
Disk location: 04-C0-00-2,0
Size (bytes): 15339008
Status:      Successful
```

If no system dump information is available, a message is displayed and no further options are provided. If system dump information is available, you will receive the following message:

Do you wish to copy the above system dump to an output device? (y/n)

Type y or n to indicate if you want to proceed. Upon proceeding, you will be provided a list of tape devices available on the system. After you select the device, the dump data is copied to the selected media.

Note: This procedure must vary on the *rootvg volume group* to gain access to the dump logical volume and other commands used to collect operating system data. Because the rootvg cannot be varied off, you are placed in a

maintenance shell after the dump copy completes, where you can perform other operating system commands or reboot the system.

Rebooting the System Menu

An option is provided on the Main Menu to **Reboot the System** if you choose not to reinstall the system at this time.

You can reboot in *normal* mode if the system was previously installed and has not been overwritten. You can reboot in *service* mode to restart the installation process. The process of selecting between normal and service mode differs depending on the *platform type*.

1. For **rs6k** and **rs6k/MP** machines, you can turn the system key between the *normal* and *service* positions before selecting to reboot. The system boots in the mode selected.
2. For **rspc** and **chrp** machines, there is no system key. The system boots in normal mode (from the first available disk) by default. To boot in service mode, follow the example instructions provided in Appendix B, “Booting a System for SysBack Installation or Maintenance”, on page B-1. However, you should refer to the documentation that accompanied your particular machine type for detailed instructions regarding system boot procedures.

The system shuts down, the screen clears, and the system reboots.

Chapter 13. Network Boot/Installation Configuration

The Sysback Network Boot/Install Configuration options create and configure a host to provide boot and optional installation services to a client host over the network.

The SysBack Network Boot functions use the BOOTP protocol to enable a client to communicate with the boot server. The client sends a BOOTP request across the network to a server. Then, the server, if configured, responds with the information that the client needs to contact that server and, subsequently, access the network boot image.

Once the client has successfully transferred the network boot image, the client uses this image to boot into maintenance mode and display the System Backup & Recovery for AIX Installation & Maintenance Main Menu.

Classic Network Boot and NIM Resource Boot

This section explains the differences between the Classic Network Boot and the NIM Resource Boot.

Classic Boot

The SysBack Classic Network Boot method used in versions earlier than 5, continues in Version 5 for environments that do not use AIX NIM (Network Installation Manager) resources.

The Classic Network Boot method relies on the / and /usr filesystems of the boot server for creating the network boot image. The boot server also fulfills other processing requirements for the client during the boot/installation process. Therefore, the boot server must meet certain requirements in order for the boot client to successfully utilize the boot server's resources. Specifically:

1. The operating system level of the boot server must be the same level as the boot client when using SysBack only to boot into maintenance mode. (The client must boot from the same level as what is currently installed.)
2. The operating system level of the boot server must be the same level as the installation/restore image used to reinstall the client machine when booting and installing the client. (The client must boot from the same level as the image to be installed.)
3. The boot server must have installed any AIX filesets required for the client to support attached hardware.

Note: If filesets are installed specifically to support a boot client, the server must be rebooted, and the network boot image updated and recreated before the client will successfully boot from the boot server.

4. The boot server must have installed kernel filesets to support the processor type (uniprocessor or multiprocessor) of the boot client regardless of whether or not the boot server is of the same processor type.

Note: If filesets are installed specifically to support a boot client, the server must be rebooted and the network boot image updated or recreated before the client can successfully boot from the boot server.

5. SysBack must be installed on the boot server.

Note: If filesets are installed specifically to support a boot client, the server must be rebooted and the network boot image updated or recreated before the client can successfully boot from the boot server.

NIM Resource Boot

The SysBack NIM Resource Boot method provides a mechanism for the user to use existing NIM **SPOT** and **LPPSOURCE** resources in combination with SysBack boot/installation operations. The NIM Resource Boot method relies on an existing NIM **SPOT** to provide the network boot image and an existing NIM **LPPSOURCE** to provide the device support that the client may need to support attached hardware. Therefore, the following requirements must be met by the NIM resources:

1. The NIM resources must be correctly configured before attempting to use them with SysBack. For more information on configuring NIM and its resources, refer to the book, *Network Installation Manager Guide and Reference*.
2. The NIM **SPOT** resource server must be the same server to which the client will send its BOOTP request.
3. The NIM **LPPSOURCE** resource server can be either the same server, or a different server, than the NIM **SPOT** resource server.
4. The boot client has been previously configured as a NIM client.
5. The NIM **SPOT** resource meets the operating system level, kernel support, and device support requirements for a boot server using the Classic Network Boot method described above.

Note: If any filesets are installed to the NIM **SPOT** resource to specifically support the boot of a particular client, the network boot image must be updated or recreated before the client will successfully boot from the boot server.

6. The NIM **LPPSOURCE** resource contains any the filesets needed to support attached hardware, or any kernel support filesets to support processor type (uniprocessor vs. multiprocessor) that the client will require and are not already contained within the backup image to be installed.
7. SysBack must be installed in the NIM **SPOT** resource. For more information on installing Sysback into a NIM **SPOT** resource, see “Installing SysBack into a SPOT Resource” on page 13-10.

Note: If SysBack is installed into a NIM **SPOT** resource to support SysBack boot clients, the network boot image must be updated or recreated before the client can successfully boot from the boot server.

Classic Network Boot

Accessing and Configuring the Classic Network Boot Menus

The Classic Network Boot menus enables the user to:

- Add or change a network boot client.
- Set network install client defaults.
- Rebuild network boot images.
- Remove a network boot/install client.

To access the Classic Network Boot menus, select **Classic Network Boot** from the Network Boot/Install Configuration menu.

Note: From a command line, type `sb_netboot`.

Configuring or Updating a Network Boot Image

The Network Boot Image exists on the Network Install Server, and is sent to the client system only upon request in order to boot the client system to the SysBack Installation and Maintenance Menus. This prevents the need to have boot media, such as a tape or diskettes, available at the client in order to perform a network install.

A separate boot image must be created for each type of network adapter to be used for the network install. The available network install adapter types are ethernet, token ring, and FDDI. A network boot image must be created for each platform type as well. For example, an `rspc` platform can boot from the same server as an `rs6k` platform, but each will use a different network boot image.

If you have applied AIX updates to your system, or have added software to support new hardware on the client, then you should update the boot image using this option. To update an existing boot image, follow the same instructions as creating a boot image for the first time. The previous image file will be overwritten, and any configured clients will begin using the new image automatically.

Cloning systems: A System Backup created on one machine can be installed on another machine with a different processor or machine type. If booting a client machine of a different machine type or with a different hardware configuration, you must have installed the device support on the server for all devices to be used by the client machine. You must also have created a separate network boot image for each platform type.

Adding or Changing a Network Boot Client

This option configures a network boot client that is to be booted from the server. This option generates the information needed to respond to the client's BOOTP request, and assigns the specific boot image that will be used to boot the client, depending on the client's network adapter and platform type. If a network boot image for this client's platform, kernel, and device type does not already exist, a boot image will be created in the `/usr/lpp/sysback/netinst/bootimages` directory.

Important Note: This option provides the client system with permission to mount the server's `/usr` filesystem in read-only mode. If you do not want the client to be permitted read-only access to the server's `/usr` filesystem once the install has completed, use the **Remove a Network Boot Client** option after installation.

If the network adapter changes on the client system, it is necessary to update the server to reflect the new adapter type and hardware address of the client machine. You can update the boot client information if already configured, using the steps for a new client.

The adapter "hardware address" refers to the physical network adapter's hardware address, which differs from adapter to adapter. By entering an adapter hardware

address, the server responds to a broadcast BOOTP request so the client system will not have to specify server information in the BOOTP menu. This option is not usually required by most systems.

To add or change a network boot client:

1. From the Classic Network Boot Menu, select **Add or Change a Network Boot Client**.

Note: From a command line, type `smit sb_cfgbootclient`.

2. Type the client hostname of the machine that will be booted from this server. The client hostname must be resolvable by the server.

Note: If changing a client already configured to this server, press F4 to get a list of previously configured clients.

3. The following screen will be displayed.

Add or Change a Network Boot Client

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

*Client hostname

*Client network adapter type

Client platform/kernel type

Server IP address

Client gateway address (optional)

Client subnet mask (optional)

Client adapter hardware address (optional)

[Entry Fields]

[sysback2.aix.dfw.ibm.c>

token ring +

rsrc +

[9.19.134.93]

F1=Help

F2=Refresh

F3=Cancel

F4=List

F5=Reset

F6=Command

F7=Edit

F8=Image

F9=Shell

F10=Exit

Enter=Do

Figure 13-1. The Add or Change a Network Boot Client Menu

The options have the following definitions:

Note: If the client selected was previously configured, the fields will retain their previous values by default.

Client Hostname (Required)

The name of the boot client. This is the hostname, or fully qualified hostname, of the client machine.

Client Network Adapter Type (Required)

The type of adapter the client uses to boot from the network boot server. The default is the first network adapter type detected by the system. The available options are:

- ethernet
- token ring
- FDDI

Client Platform/Kernel Type (Required)

The type of architecture/platform and the processor type of the client to boot from the network install server. The default is the server's platform and kernel type.

The available options are:

chrp Common Hardware Reference Platform

chrp/MP

Multiprocessor Common Hardware Reference Platform

rs6k RISC System/6000 (uniprocessor)

rs6k/MP

Multiprocessor RISC System/6000

rspc PCI-based (PC) RISC System/6000 (uniprocessor)

rspc/MP

Multiprocessor PCI-based (PC) PC RISC System/6000

The first part of the selection is the platform type. The second part (/MP) indicates the kernel type. If the kernel type portion is omitted, a uniprocessor (single processor) kernel is used.

Server IP Address (Required)

The IP Address for the boot server. The default is the current IP address of the system. Change this value only if the boot server has multiple IP addresses and the default supplied is not desirable.

Client Gateway Address (Optional)

The network address of the gateway that the client must use to reach this server, if any.

Client Subnet Mask (Optional)

The network mask, if required, that the client must use to communicate on the network.

Client Adapter Hardware Address (Optional)

The client's network adapter hardware address. This value is required for only certain RSPC platform clients or if the user desires to broadcast the BOOTP request without completing the server information. Do not use this field for clients that communicate with the server through a gateway.

4. Once all entries are completed, press Enter to confirm selections and execute your choice.

Note: If a boot image for the client's adapter, platform, and kernel combination does not already exist, a boot image is created automatically when adding the boot client.

Setting the Network Install Client Defaults

If you install a client system from a network install server, you can customize installation to reduce, or even eliminate, the amount of information a user must enter to initiate the installation of the client machine. The complete elimination of all prompts is referred to as a "no-prompt install" or an "unprompted installation". This is accomplished by setting all installation information that the user is normally prompted for before actually performing the network installation.

Configure the client as a network boot client before you set the network installation defaults for that client.

To set the Network Install Client Defaults:

Note: You may also access this same menu by using the following SMIT paths:

```

smitty sysback          Sysback Program Defaults
Change Sysback Program Defaults      Change Sysback Tape
Defaults                          Change Sysback CD/DVD Boot Defaults
                                Set Network Install Defaults

```

1. From the Classic Network Boot Menu, select **Set Network Install Client Defaults**.

Note: From a command line, type `smit sb_cfginstclient`.

2. Highlight the client and press Enter.
3. The following screen is displayed.

Set Network Install Client Defaults

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

[TOP]	[Entry Fields]
*Client hostname	sysback2.aix.dfw.ibm.c>
Perform no-prompt installation?	no +
Debug Logging?	no +
THE FOLLOWING ARE REQUIRED FOR NOPROMPT INSTALL:	
Console Device Name	<input type="text"/>
Console Terminal Type (if ascii)	<input type="text"/>
Non-rootvg Volume Group Option	Restore rootvg only +
Restore Device or File	<input type="text"/> +
Backup Sequence Number (if tape)	<input type="text"/> #
Remove Sysback from foreign client after install?	no +
Remove Network Config from foreign client?	no +
THE FOLLOWING ARE REQUIRED ONLY IF THE INSTALL SERVER DIFFERS FROM THE BOOT SERVER:	
[MORE...11]	

F1=Help
F5=Reset
F9=Shell

F2=Refresh
F6=Command
F10=Exit

F3=Cancel
F7=Edit
Enter=Do

F4=List
F8=Image

Figure 13-2. The Set Network Install Client Defaults Menu

The options have the following definitions:

Note: If the client selected was previously configured, the fields retain their previous values by default.

Client Hostname

This field cannot be changed; it was populated from input of the previous menu screen.

Perform No-Prompt Installation

Specifies if the client to be installed will be prompted. If this field is set to “no”, the installation menus will appear after a network boot. Otherwise, the installation occurs after the network boot without prompting the user, provided that all required information for the installation is also provided. The default is “no”.

Debug Logging

Indicates whether or not to turn on debug logging operations for troubleshooting network boot and installation problems. The default is “no”.

Console Device Name

Enter the name of the console device prior to installation to prevent displaying the prompt prior to the installation menus. The console device can be either an LFT (graphical display) or TTY (ascii display) device. Examples are `/dev/lft0` or `/dev/tty0`. Also, if an LFT device exists on the client, it can also be selected by typing `/dev/console`. The default is “none/blank”.

Note: The display must be selected, even for a no-prompt install. This lets you receive any error or warning messages and prompts you if the default information provided is insufficient to complete the installation.

Console Terminal Type (if ascii)

If the console device is an ascii terminal, or TTY device, you must select a specific terminal type. This ensures that installation menus, if required, are displayed with the correct terminal emulation. Enter the device type or press F4 to display a list of all terminal types defined on the server and select from the list. Examples of common terminal types are `ibm3151`, `tvi925` and `vt100`. The default is “none/blank”.

Non-rootvg Volume Group Option

The default is “Restore Rootvg Only”. The following is a description of the options for this field.

Restore Rootvg Only

Only the rootvg volume group is created and restored from the media, even if there were other volume groups defined on the backup. At the end of the install, only the rootvg volume group will be defined on the system.

Restore All VGs

All volume groups that are included on the backup media are created and restored. Volume groups that are defined on the original system but whose data was not included on the backup are created but data is not restored.

Import Non-Rootvgs

The rootvg volume group is created and restored. All other volume groups, if any, are imported from disks on the client. This option assumes that the non-rootvg volume groups already exist on the client. Use this option when restoring the rootvg volume group after a system failure where no other volume groups were affected.

Restore Device or File

The options shown are made available using the **Add or Change Client Host Access to this Server** option under the Remote Services menu. You must select an option from this list to prevent being prompted for an installation device or file during the installation process. The default is “none/blank”. For more information on defining these resource, see Chapter 8, “Remote Services”, on page 8-1.

Backup Sequence Number (if tape)

If the client is installed from tape, and the system backup to be

installed is not the first system backup on the tape, enter the backup sequence number. This number must be between 1 and the total number of system backups on the tape media. The default is "none/blank".

Remove SysBack from Foreign Client After Install

Indicates whether or not to remove the SysBack program from the system after installation. Choose "yes" when you have not purchased a license for the client that will be installed. The default is "no".

Note: If you are installing a backup on an LPAR capable machine, that was made from another partition in that same machine, this prompt will not occur. However, if you would like to remove the product from the new partition, you may configure SysBack to do so using the Utilities menu option described in "Remove SysBack Programs After Install" on page 12-15.

Remove Network Configuration from Foreign Client

Indicates whether or not to remove network specific information required to configure the host to the network. Choose "yes" when the machine installed was cloned from a backup image of a machine that is still present on the network. The default is "no".

Note: If you are installing a backup on an LPAR capable machine, that was made from another partition in that same machine, this prompt will not occur. However, if you would like to remove the product from the new partition, you may configure SysBack to do so using the Utilities menu option described in "Removing the Network Configuration" on page 12-11.

Install Server IP Address

The address of the installation server. If the boot server is also the installation server, do not change this option. If the backup media from which the client is installed exists on a different server, enter the IP address of the installation server. The default is the boot server's IP address.

Gateway Address

The address of the boot server. If the boot server is also the installation server, do not change this option. If the client is installed from server other than the network boot server and a different gateway address is required to reach the installation server, enter that gateway IP address. The default is the boot server's gateway address.

Network Device Name

If the client is installed using a network adapter different than it was booted from, enter the device name of the network adapter here. The default is "none/blank".

Subnet Mask

If the client is installed using a network different than it was booted from, enter the subnet mask, if any, required for the network adapter to contact the installation server. The default is "none/blank".

Token-Ring Speed (if applicable)

If the installation server uses a different network adapter, and the network adapter is token-ring, select the correct token-ring speed. If the boot server is also the installation server, do not set this option. The default is "none/blank".

Ethernet Interface (if applicable)

If the install server uses a different network adapter, and the network adapter is ethernet, select the correct interface type. If the boot server is also the installation server, do not set this option. The default is "none/blank".

Ethernet Connection Type

If the install server uses a different network adapter, and the network adapter is ethernet, select the correct connection type. If the boot server is also the installation server, do not change this option. The default is "none/blank".

Post-Install Script

To assign a specific post-install script to run at the end of the installation process, enter the fully qualified path and the name of the post-install script file. The file must exist on the installation server and be readable by the client during installation. Refer to Appendix D, "Creating Scripts for Customizing the System Backup and Install Process", on page D-1 for additional information on post-install scripts. The default is "none/blank".

LVM Information file

To use a customized LVM information file during client installation, enter the fully qualified path and name of the LVM information file in this field. The LVM information file must contain information that is compatible with the client. The file must exist on the installation server and be readable by the client during installation. For additional information on creating an LVM Information file, see Chapter 16, "Utilities", on page 16-1. The default is "none/blank".

4. Once all entries are complete, press Enter to confirm selections and execute your choices.

Rebuilding Network Boot Images

If software is updated or installed in the boot source, you must update or rebuild the boot image. For the Classic Boot method, the source would be the /usr of the boot server. For the NIM Resource Boot method, the source would be the NIM SPOT resource.

To build a network boot image:

1. From either the Classic Boot Method or NIM Resource Network Boot Method menu, select **Rebuild Boot Images**.

Note: From the command line, type `smit sb_updboot image`

2. Press F4 to list the image and select an image to update.
3. Press Enter to confirm your choices.

This option can be used to update both Classic method or NIM Resource method boot images.

Removing a Network Boot/Install Client

This option removes a network boot client and all information configured for network installation from the boot server. Use this option after the client installation is complete. It prevents the client system from remotely mounting the /usr filesystem in read-only mode from the server. If there is no reason to prevent the client system from mounting /usr from the server, the client configuration may

be retained, enabling the client machine to boot from the server as needed for re-installation or to perform system maintenance.

To remove a network boot client:

1. From the Classic Network Boot Menu, select **Remove a Network Boot Client**.

Note: From a command line, type `smit sb_ucfgbootclient`.

2. Highlight the client and press Enter.
3. Once all entries are complete, press Enter to confirm selections and execute your choices.

NIM Resource Boot

Accessing and Configuring the NIM Resource Menus

The NIM Resource Boot menus let you:

- Install SysBack into a **SPOT** resource.
- Query for SysBack installation in a **SPOT** resource.
- Add or change a network boot client.
- Set network install client defaults.
- Rebuild network boot images.
- Remove a network boot/install client.

To access the NIM Resource Boot menu, select **NIM Resource Boot** from the Network Boot/Install Configuration menu.

Note: From a command line, type `smit sb_nimboot`.

Installing SysBack into a SPOT Resource

The NIM **SPOT** resource must have SysBack installed in order for the SysBack boot and installation process to succeed. It is important that SysBack is installed into the NIM SPOT using this utility rather than NIM commands. SysBack has special binaries for different levels of AIX. Using this utility to install the product ensures that the correct binaries are applied based on the AIX version of the SPOT rather than the AIX version of the system where the SPOT resides.

Note: When performing a network boot in order to restore from a TSM server, you must install the TSM API client filesets using NIM commands. This utilities is designed to support only the installing of the SysBack product into the SPOT.

Use the **Install SysBack into a Spot Resource** for a first time installation of SysBack into a NIM **SPOT** resource or to update the level of SysBack installed in that **SPOT** resource.

To install SysBack into a NIM **SPOT** Resource:

1. From the NIM Resource Boot menu, select **Install SysBack into a Spot Resource**.

Note: From a command line, type `smit sb_nimspotcust`.

2. Type the device or directory name where the SysBack install image resides.

3. The following screen is displayed.

Install Sysback into Spot Resource

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

*INPUT device/directory for software

*NIM SPOT Resource Name

*NIM LPP Source Name

OVERWRITE Same or newer version?

[Entry Fields]

/usr/sys/inst.images

no

+

+

+

F1=Help

F2=Refresh

F3=Cancel

F4=List

F5=Reset

F6=Command

F7=Edit

F8=Image

F9=Shell

F10=Exit

Enter=Do

Figure 13-3. The Install Sysback into Spot Resource Menu

The options have the following definitions:

INPUT device / directory for software

This field cannot be edited; its contents are specified from a previous selector screen.

NIM SPOT Resource Name

The NIM object name for the **SPOT** resource where SysBack will be installed. Press F4 to get a list of previously configured NIM **SPOT** resources.

NIM LPP Source Name

The NIM object name for the **LPPSOURCE** resource that supplies the SysBack image. Press F4 to get a list of previously configured NIM **LPPSOURCE** resources.

Note: The NIM **LPPSOURCE** resource specified should contain AIX filesets of the same AIX level as the **SPOT** resource used to install the client. For example, if the **SPOT** resource supplies boot information for an AIX 4.3.3 system, the corresponding **LPPSOURCE** should contain AIX filesets that are also at the AIX 4.3.3 level. This is not a requirement for any optional software packages installed into the **LPPSOURCE**; each package can have its own operating system compatibility requirements. The level of SysBack contained in the **LPPSOURCE** can be any level supported by the AIX level of the specified **SPOT** resource.

OVERWRITE Same or newer version?

Set this option to Yes if you want to reinstall the same, or an older version of SysBack, than exists in this SPOT resource.

- Once all entries are complete, press Enter to confirm selections and execute your choices.

Note: The image is first copied from the specified input device or directory and then copied to the specified **LPPSOURCE** before it is installed to the specified **SPOT** resource.

Querying for SysBack Installation in SPOT Resource

This option can be used to determine if SysBack is installed in to a NIM SPOT resource and, if so, at what level.

To query for installation:

1. From the NIM Resource Boot menu, select **Query for SysBack Installation in SPOT Resource**.

Note: From the command line, type `smit sb_querysb`.

2. Press Enter.

Adding or Changing a Network Boot Client

This option configures a network boot client to be booted from the server. This option generates the information necessary to boot the client using the specified NIM SPOT resource. This option also automatically generates a boot image for the specified client using the named NIM SPOT resource. SysBack obtains the information regarding the client's platform and kernel type from the previously configured NIM machine object for that client.

To update the client's boot image after installing or updating the software into the NIM SPOT resource used by the client, repeat this process to change and update the client's boot image.

To add or change a network boot client:

1. From the NIM Resource Boot menu, select **Add or Change a Network Boot Client**.

Note: From a command line, type `smit sb_nimaddclient`.

2. Highlight the client and press Enter.
3. The following screen is displayed.

Add or Change a Network Boot Client

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

*NIM Client Name *NIM SPOT Resource Name *NIM LPP Source Name	<div style="text-align: center; margin-bottom: 5px;">[Entry Fields]</div> <div style="display: flex; align-items: center;"><div style="border: 1px solid black; width: 100px; height: 1.2em; margin-right: 5px;"></div><div style="margin-right: 5px;">sysback2</div><div style="margin-right: 5px;">+</div><div style="border: 1px solid black; width: 100px; height: 1.2em; margin-right: 5px;"></div><div style="margin-right: 5px;">+</div></div>
---	---

F1=Help
F5=Reset
F9=Shell

F2=Refresh
F6=Command
F10=Exit

F3=Cancel
F7=Edit
Enter=Do

F4=List
F8=Image

Figure 13-4. The Add or Change a Network Boot Client Menu

The options have the following definitions:

NIM Client Name

The NIM machine object name for the boot client. This field cannot be edited; it was generated from input on the previous selector screen.

NIM SPOT Resource Name

The NIM **SPOT** name that SysBack will use to create the boot image for the client named above.

Note: The requirements described in the NIM Resource Boot discussion in “Classic Network Boot and NIM Resource Boot” on page 13-1 must be followed.

NIM LPP Source Name

The NIM **LPPSOURCE** resource that SysBack uses to obtain necessary device support for the boot client when cloning from a backup image that does not contain the device support needed for this client.

4. Once all entries are complete, press Enter to confirm selections and execute your choices.

Rebuilding Network Boot Images

If software is updated or installed in the boot source, you must update or rebuild the boot image. For the Classic Boot method, the source would be the /usr of the boot server. For the NIM Resource Boot method, the source would be the NIM **SPOT** resource.

To rebuild a network boot image:

1. From either the Classic Boot Method or NIM Resource Network Boot Method menu, select **Rebuild Boot Images**.

Note: From the command line, type `smit sb_updbootimage`.

2. Press F4 to list the images and select an image to update.

Note: Although you can select individual boot images to rebuild, all the boot images associated with a single NIM **SPOT**, even if you choose only one image.

3. Press Enter to confirm your choices.

Removing a Network Boot/Install Client

This option will remove a network boot client and all information configured for network installation from the boot server/resources.

This affects only SysBack configurations and does not change any previously defined NIM resource information.

To remove a network boot/install client:

1. From the NIM Resource Boot menu, select **Remove a Network Boot/Install Client**.

Note: From a command line, type `smit sb_ucfgbootclient`.

2. Highlight the client and press Enter.
3. Press Enter to confirm your choice.

Initiating an SP Node Boot and Install

This menu option enables the user to initiate the network boot sequence for an SP node because the RS/6000 Scalable POWERParallel systems have special requirements for installing and cloning.

For a complete explanation on how to access and use this menu option, see Chapter 14, “RS/6000 Scalable POWERParallel Systems® (SP) Boot and Install Utilities”, on page 14-1.

Chapter 14. RS/6000 Scalable POWERParallel Systems® (SP) Boot and Install Utilities

The RS/600® SP® systems, unlike the non-SP RS/6000 systems, have special requirements for installing and cloning. The RS/6000 SP System is comprised of a Control Workstation (CWS) and one or more nodes. Each node and the CWS are independent machines that work together using a complex system of network daemons, configuration files, and hardware. The nodes do not have floppy drives or LED panels consistent with non-SP RS/6000 systems.

SysBack backup and restore operations on the SP are identical to non-SP RS/6000 systems. When these operations are performed across network interfaces, not to locally attached tape devices, the setup and configuration requirements do not differ from the non-SP systems. However, the installation process requires some additional considerations.

This chapter provides the information necessary to fully exploit SysBack installations in an SP environment.

Advantages of the SysBack SP Boot and Installation Utilities

In previous versions of SysBack, the SP administrator had to perform several specific SP installation activities manually. For example, if a node was reinstalled, the administrator had to set the node to “disk” in the SDR to enable SysBack to complete the installation process rather than PSSP. The node would have to be manually customized and the PSSP script run. If the node was cloned from the image of another node, further actions were required, including updating the `/etc/niminfo` file and other configuration files.

In SysBack Version 5, the product works with PSSP to handle these SP system specific issue during the node’s installation process. SysBack sets the SDR’s **bootp_response**, run **setup_server**, perform node conditioning, and runs the **PSSP** script. Reinstallation of a node using the SysBack SP boot and installation utilities results in a fully recovered node.

The administrator continues to perform the usual activities associated with preparing an SP node to be installed, as well as, the post-installation application and network specific activities.

SysBack expects to use the same NIM **SPOT** and **LPPLOURCE** that is used when the node is installed with a **mksysb** image using the default SP installation process. An indication that the node has been properly prepared for installation is that the node can be successfully installed with the SP/NIM designated **mksysb** image using the standard PSSP installation process.

For more information on how to work with a nodes NIM **SPOT** and **LPPSOURCE**, see the publications:

- *PSSP Command and Technical Reference, Volume 2*
- *PSSP Administration Guide*

How SysBack works with NIM on the SP System

NIM, Network Installation Manager, is an AIX facility used for the installation and configuration of software through a network interface. SysBack Version 5 contains a new network boot/install configuration option that uses NIM Resources to provide the boot image and the location of device support when an image is cloned.

SysBack can now use an existing, previously configured NIM **SPOT** and **LPPSOURCE** resource for installation. See Chapter 13, “Network Boot/Installation Configuration”, on page 13-1 for more information.

The SysBack SP boot/install utilities couple with the NIM Resource Network Boot features to work with the SP.

Unlike previous versions of SysBack, the boot and installation of a SP node is now initiated using the **Initiate SP Node Boot and Install** menu option, or the **spsbboot** command. The Classic Network Boot options are no longer recommended for SP node boot/installation.

For information on the Network Installation Manager (NIM), see the book, *Network Installation Manager Guide and Reference*.

Special Assumptions

Assume the following of SysBack:

- The SP administrator understands and has executed all SP specific installation preparations before installing a node using SysBack.
- The SP administrator has properly set up and configured the NIM environment for the SP complex.
- SysBack will use the same NIM **SPOT** and **LPPSOURCE** resources during the boot/install process as a standard PSSP installation.
- You have installed SysBack into the appropriate NIM **SPOT** resource. See Chapter 13, “Network Boot/Installation Configuration”, on page 13-1 for more information on installing SysBack into the NIM **SPOT** resource.
- You have added the node to be booted/installed as a SysBack network boot client before initiating the boot/installation process.
- The SP administrator has installed the necessary device support into the **LPPSOURCE** before installation. SysBack now automatically installs necessary device support not contained in the backup image when cloning that image to a new SP node through the configured NIM **LPPSOURCE**.
- You initiate the SP node boot/installation using the SysBack menu option **Initiate SP Node Boot and Install** or the **sbspboot** command.
- The SP administrator can perform and execute any application, SP, or Network specific post-installation activities. This is especially important after cloning an image to a new node.

Accessing the SP Boot and Install Options

You can access the SP Boot and Install menu one of two ways.

Option 1

1. From the SysBack Main Menu, select **Configuration Options**.

Note: From a command line, type `smit sb_config`.

2. Select **Network Boot/Install Configuration**.

Note: From a command line, type `smit sb_netboot_choice`.

3. Select **Initiate SP Node Boot and Install**.

Note: From a command line, type `smit sb_spboot`.

Option 2

1. From the SysBack Main Menu, select **Backup & Recovery Options**.

Note: From a command line, type `smit sb_opt`.

2. Select **Initiate SP Node Boot and Install**.

Note: From a command line, type `smit sb_spboot`.

Completing the Initiate SP Node Boot and Install Menu

To initiate the SP node boot and installation:

1. Access the menu using one of the two options explained in the previous section.
2. At the Select a NIM Client screen, select the desired SP node and press Enter.
3. The following screen is displayed:

Initiate SP Node Boot and Install

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

	[Entry Fields]	
*SP Node Name	sysback2	
NIM SPOT Resource Name	<input type="text"/>	+
NIM LPP Source Name	<input type="text"/>	+
XWindow's Display	<input type="text"/>	+

F1=Help
F5=Reset
F9=Shell

F2=Refresh
F6=Command
F10=Exit

F3=Cancel
F7=Edit
Enter=Do

F4=List
F8=Image

Figure 14-1. The Initiate SP Node Boot and Install Menu

Unprompted and Prompted Installations

SysBack installations are prompted by default. When booting to the SysBack Maintenance Menu to begin an installation, you can install from a different installation device, modify logical volume and volume group attributes, or access other utilities. See Chapter 12, “System Installation and Maintenance”, on page 12-1 for information on these options.

SysBack also lets you define installation defaults to eliminate most prompts during installation. This is called an “unprompted install”. See Chapter 16, “Utilities”, on page 16-1 for more information on setting installation defaults. Also see Chapter 12, “System Installation and Maintenance”, on page 12-1 for more information on unprompted installations.

SP installations in a non-SysBack environment are generally unprompted. Therefore, the SP administrator must set up the installation defaults prior to initiating an unprompted SysBack installation.

By default, a console window or a **s1term** window does not automatically open during an unprompted SysBack installation. However, you can monitor the progress by opening a **s1term** using one of two methods:

1. From the SP control workstation, type the command

```
s1term <frame#><slot#>
```

where `frame#` represents the node’s frame and `slot#` represents the node’s slot.

Note: This opens a read-only terminal. Adding `-w` to the `s1term` command results in a writable terminal.

2. Select **Open TTY** from the HW Perspectives view of the node using the **perspectives** command from the SP Control Workstation.

When you install on one node an image created on a different machine (called “cloning”), a prompted install is recommended.

Troubleshooting Tips

If problems arise during installation, you can use the following resources:

- For unprompted installs, manually open a `s1term` (console window) to determine the progress or failure messages of the installation.
- For boot problems, initiate Manual Node Conditioning of the SP node using the **SP nodecond** command. For details on executing this process, see the following publications or contact your SP System Technical Support Organization:
 - *PSSP Command and Technical Reference, Volume 1*
 - *PSSP Diagnosis Guide*
 - *PSSP Administration Guide*
- Use the HW Perspective view of the node to monitor the progress of the boot/installation. This view can be accessed using the **SP perspectives** command from the SP Control Workstation.

Chapter 15. Integrating to IBM Tivoli Storage Manager

SysBack version 5.6 and later allows for the storage of backup objects into an IBM Tivoli Storage Manager server. Backups to a TSM server may be manipulated like any other SysBack backup. They may be listed, verified, restored, and used for system reinstallation.

Combining the SysBack backup, restore, and network boot / install functions with a TSM server provides bare metal recovery capability for TSM configurations. SysBack will back up and recover a system's volume group, logical volume, and file system information. Optionally, SysBack will back up any non-rootvg data specified. SysBack may be used as a stand alone backup and recovery solution. However, some customers may opt to use SysBack simply to recover the rootvg volume group and then use TSM to backup and manage other user data.

Prerequisites, Limitations, and Exclusions

The hardware and operating system requirements for storing backups into a TSM server are the same as the base product as defined in "System Requirements" on page 1-1. The following additional requirements are specific to interactions with TSM:

- A previously configured TSM server must be at level 5.1.5 or higher
- The 32-bit TSM API client must be installed and at level 5.1.5 or higher
- The TSM node name used for SysBack backups must be registered on the TSM server and configured to use the `passwordaccess generateoption`.
- Only JFS and JFS2 file systems are supported for all of the backup types
- The File / Directory backup type may also be used to backup CD-ROM and NFS file systems
- All backup, restore, list, verify, and query operations must be performed as the root user

The following limitations and exclusions apply to interaction with TSM:

- SysBack should not be used to backup TSM HSM managed file systems. You will need to explicitly specify any HSM managed file system in the SysBack exclude list. For detailed information on SysBack exclude lists, please refer to Chapter 9, "Exclude Lists", on page 9-1.

Note: Using SysBack to back up HSM managed file systems will cause all of the migrated data to be recalled for the backup operation. This could cause lengthy backup times. Also, there may not be enough space in the file system to recall all of the migrated data. Use the TSM Backup / Archive Client to backup HSM file systems instead.

- LAN Free backups are not supported
- COMMMethod TCPIP is the only supported TSM communication method
- GPFS file systems are not supported

Note: The TSM Backup / Archive Client supports the backup of GPFS file systems.

- Veritas file systems are not supported

- AFS and DFS file system structures can not be recreated from backups. If the root user has the appropriate AFS or DFS permissions, then SysBack can backup the data.

Note: The TSM Backup / Archive Client supports the backup of AFS and DFS file systems.

- Compression should not be set from within the SysBack backup commands when the backup destination is a TSM server. Compression of data is controlled through TSM configuration options.
- Files, directories, file systems, or logical volumes that you would like excluded from backup processing must be defined in the SysBack exclude list. TSM exclude processing does not apply to this backup process. For more information on defining SysBack exclude lists, please refer to Chapter 9, “Exclude Lists”, on page 9-1.

Basic Setup and Configuration Tasks

In order to perform backup, list, verify, query, or restore operations with a TSM server, you must perform the following configuration tasks:

Register a TSM Node

Before you may perform any communications with a TSM server, you must first register a TSM node and define a password. For example, you could type the following TSM server command via the TSM Administrative Client interface:

```
dsmadmcl> register node lasher password domain=special
```

Note: There are several options available when registering a node. For more detailed information related to registering nodes to a TSM server, please refer to the *IBM Tivoli Storage Manager for AIX: Administrator's Guide (GC32-0768)* or the *IBM Tivoli Storage Manager for AIX: Administrator's Reference (GC32-0769)*.

The password will be initialized when the TSM virtual device is created. If your password is already initialized, such as when you are using the same node name as your TSM Backup / Archive Client, it will be necessary for you to provide that password when creating the virtual device definition.

Install the API Client

You must install the version 5.1.5 (or later) TSM 32-bit API client for use with SysBack operations.

Note: Please refer to the IBM Tivoli Storage Manager README.API file for detailed installation instructions.

Configure the TSM Client System Options File

You must add, update, or select an existing server stanza in the `/usr/tivoli/tsm/client/api/bin/dsm.sys` file. Operations between SysBack and TSM require at least this minimum information in the **dsm.sys** file:

```
*****
* Tivoli Storage Manager                                     *
* Sample Client System Options file for AIX and SunOS (dsm.sys.smp) *
*****
```

```
* This file contains the minimum options required to get started using TSM. Copy the * dsm.sys.smp to
* If your client node communicates with multiple TSM servers, be sure to add a stanza, * beginning w
```

```
SErvername lasher_main
NODename lasher
COMMMethod TCPIP
TCPPort 1500
TCPSeveraddress tsmserver.your.domain.com
PASSWORDAccess generate
```

The following TSM Client Options are allowed with IBM Tivoli Storage Manager for System Backup and Recovery:

- COMMMethod
- COMMRESTARTDuration
- COMMRESTARTInterval
- COMPRESSAlways
- COMPRESSIon
- FROMNode
- INCLexcl

Note: Only 5 Include statements are supported in this file. Please see the section “Binding and Rebinding Backups to TSM Management Classes” on page 15-17 for details.

- INCLUDE

Note: Only 5 Include statements are supported for backup processing. Please see the section “Binding and Rebinding Backups to TSM Management Classes” on page 15-17 for details.

- MAILprog
- NODename
- PASSWORDAccess

Note: Only the generate value is supported with this option

- PASSWORDDIR
- SErvername
- TCPBuffsize
- TCPNodelay
- TCPPort
- TCPSeveraddress
- TPCPWindowsize

Note: For more detailed information on configuring the **dsm.sys** and **dsm.opt** files, and an explanation of the uses for each of the referenced options, please refer to the *IBM Tivoli Storage Manager for Unix: Backup - Archive Clients Installation and User's Guide (GC32-0789)*

Set TSM Environment Variables

The TSM API client provides the following environment variables:

- DSML_CONFIG - The fully qualified name for the client options file usually named dsm.opt. Setting this variable is not supported with SysBack. SysBack will always set this variable to **/usr/lpp/sysback/tsm/dsm.opt.tsmXX** where **X** represents the TSM virtual device number.

- **DSML_DIR** - The path that contains the `dsm.sys`, `dsmtca`, and the `en_US` subdirectory. Setting this variable is not supported with SysBack. SysBack will always look to the default API installation directory of `/usr/tivoli/tsm/client/api/bin` to locate these items in order to allow the bare metal recovery functions.
- **DSML_LOG** - The path that points to the API error log. You may configure this variable to designate the location and filename of the API error log. If this variable is not set, the API error log for SysBack operations will be located in `/usr/lpp/sysback/sbtsmerror.log`.

Note: This does not log the output of the SysBack command processing. This only logs the information for the API communications between the SysBack command processing and the TSM server. For more information related to process logging, please refer to the section “Problem Determination” on page 15-26.

Create the TSM Virtual Device

For detailed information related to the TSM virtual device, please refer to the section “Creating, Listing, Changing, and Removing the TSM Virtual Device for SysBack”

Additional Configuration for Bare Metal Recovery

In order to perform a bare metal restore from a SysBack backup stored in a TSM server, you must execute the following configuration tasks:

- Configure operations for the backup, list, verify, query, and restore tasks as explained previously.
- Configure a SysBack Network Boot Client as explained in Chapter 13, “Network Boot/Installation Configuration”, on page 13-1.
- Configure the TSM Network Install Client Defaults as explained in “Configuring Network Boot Options for a TSM Bare Metal Recovery” on page 15-18.

Creating, Listing, Changing, and Removing the TSM Virtual Device for SysBack

All backup, restore, list, verify, and query operations communicate with the designated TSM server via a SysBack TSM Virtual Device. A virtual device allows you to logically define a TSM server for communications with SysBack operations.

Creating a TSM Virtual Device

To access the TSM Virtual Device configuration menus:

1. Log in as the root user.
2. Type **smitty sysback** and press Enter.
3. Select **TSM Configuration** and press Enter.

The following screen is displayed:

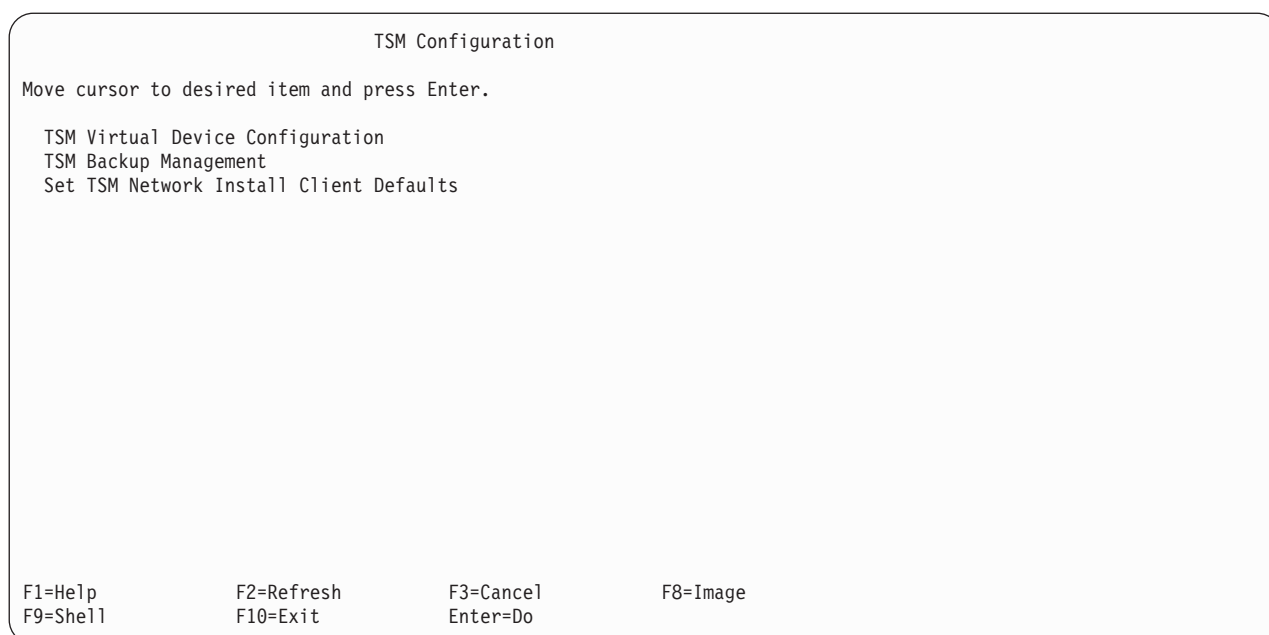


Figure 15-1. The TSM Configuration Menu

4. Select **TSM Virtual Device Configuration** and press Enter.
The following screen is displayed:

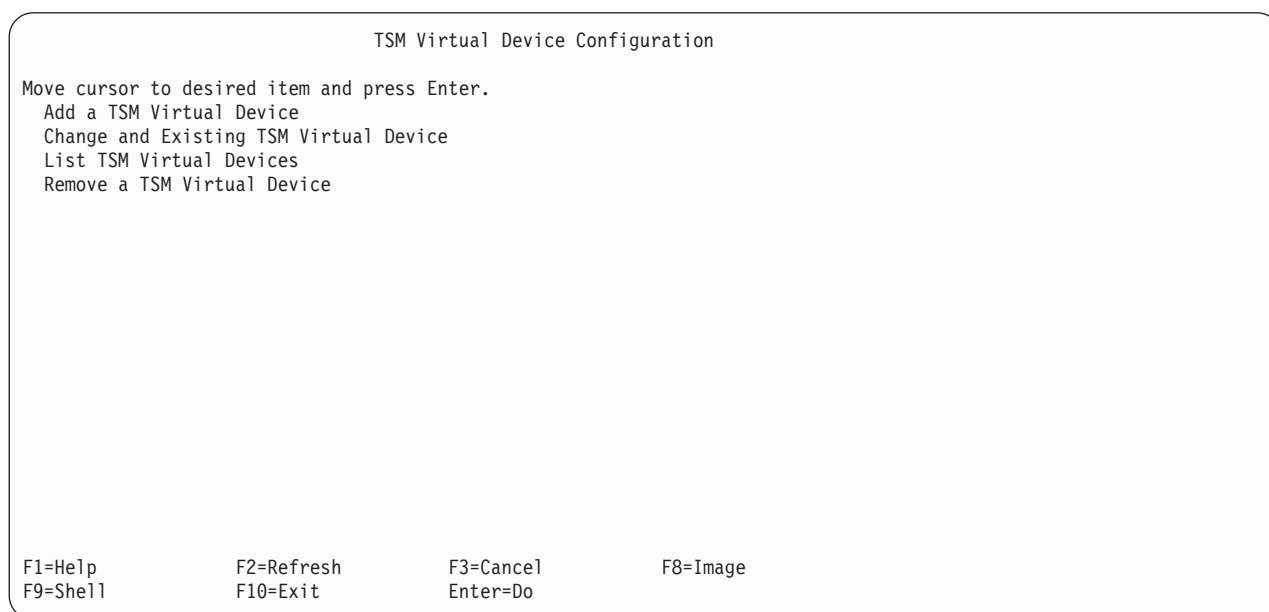


Figure 15-2. The TSM Virtual Device Configuration Menu

5. Select **Add a TSM Virtual Device** and press Enter.
6. Highlight the desired TSM server name stanza when prompted at the **Select a TSM Server** dialogue and press Enter.

Note: The list of TSM server name stanzas is generated from the contents of the `/usr/tivoli/tsm/client/api/bin/dsm.sys` file.

The following screen is displayed:

```

Add TSM Virtual Device

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

TSM Server Name      [Entry Fields]
Client Node Password  lasher1_main
                     []

F1=Help      F2=Refresh      F3=Cancel      F4=List
F5=Reset     F6=Command     F7=Edit       F8=Image
F9=Shell     F10=Exit      Enter=Do

```

Figure 15-3. The Add TSM Virtual Device Menu

Listing a TSM Virtual Device

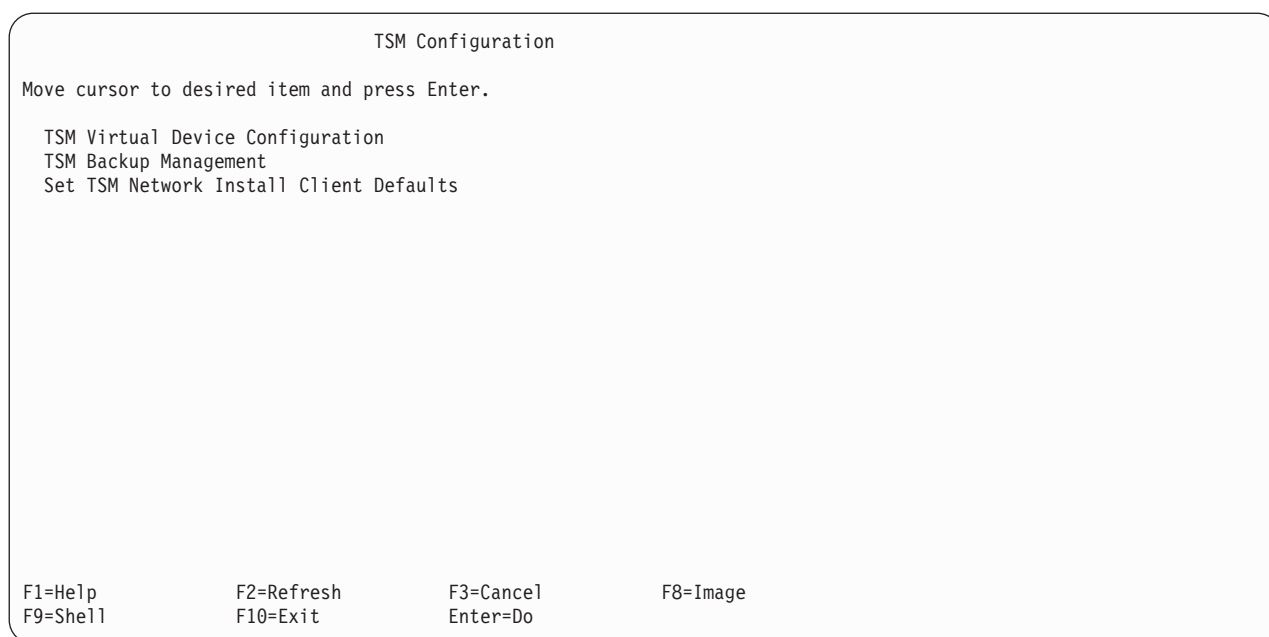


Figure 15-4. The TSM Configuration Menu

4. Select **TSM Virtual Device Configuration** and press Enter.
The following screen is displayed

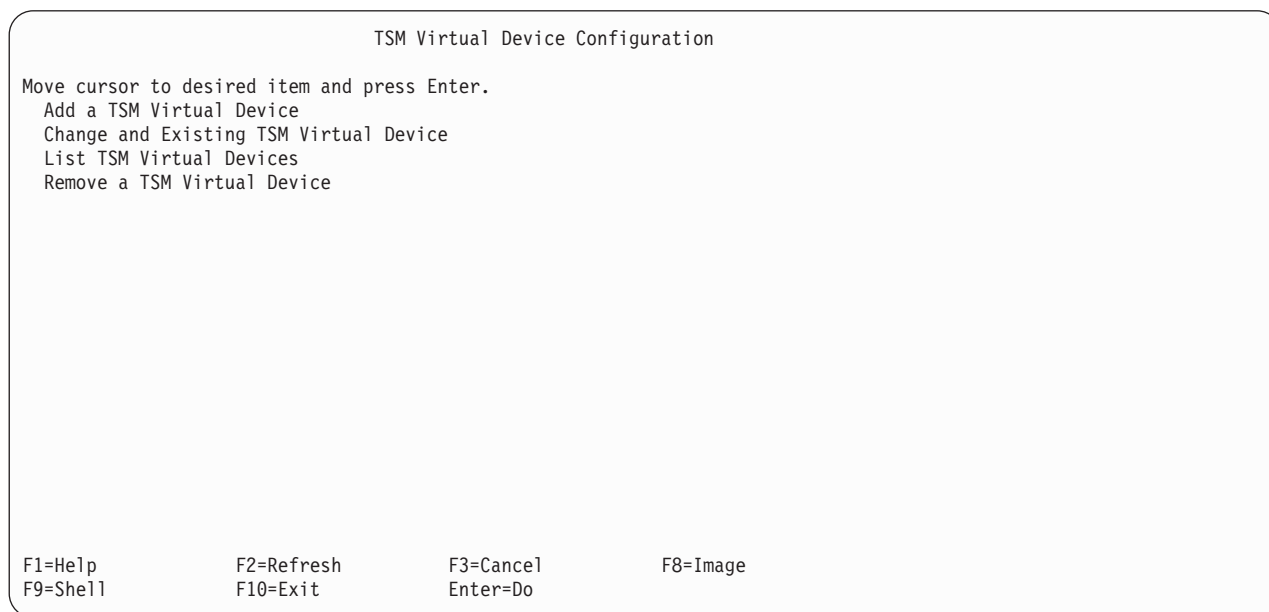


Figure 15-5. The TSM Virtual Device Configuration Menu

5. Select **List TSM Virtual Devices** and press Enter.

The list will show TSM Virtual Device name and the corresponding TSM server name stanza associated with it.

Changing the TSM Virtual Device

To access the TSM Virtual Device configuration menus:

1. Log in as the root user.

2. Type **smitty sysback** and press Enter.
 3. Select **TSM Configuration** and press Enter.
- The following screen is displayed:

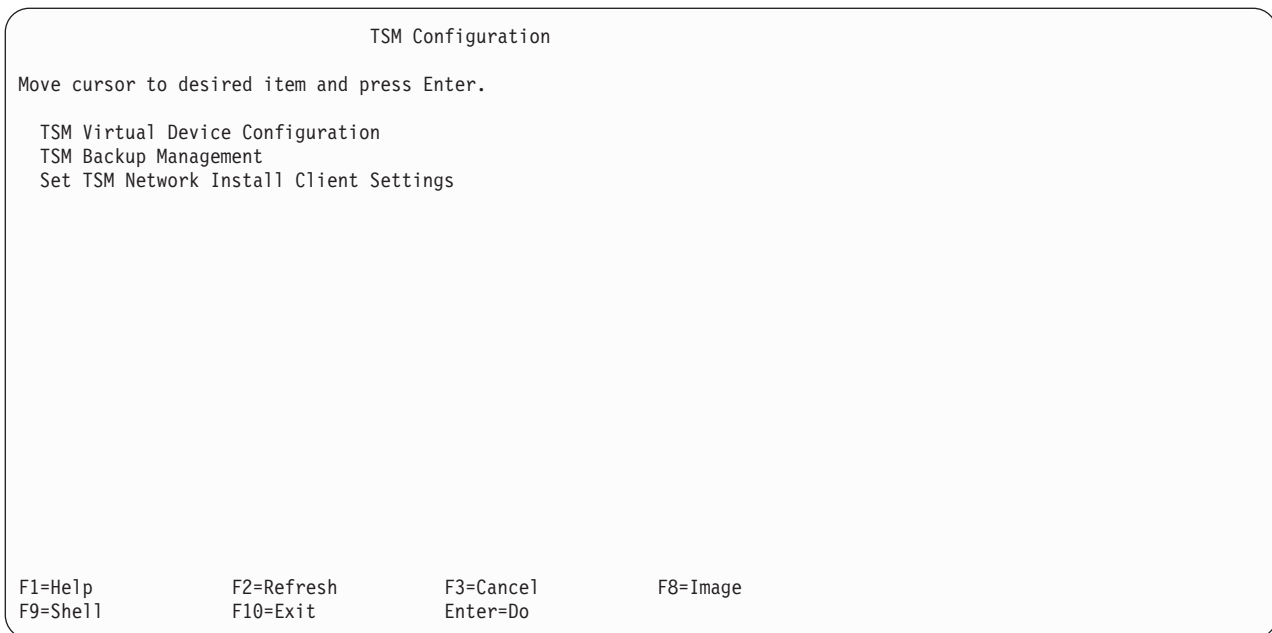


Figure 15-6. The TSM Configuration Menu

4. Select **TSM Virtual Device Configuration** and press Enter.
- The following screen is displayed:

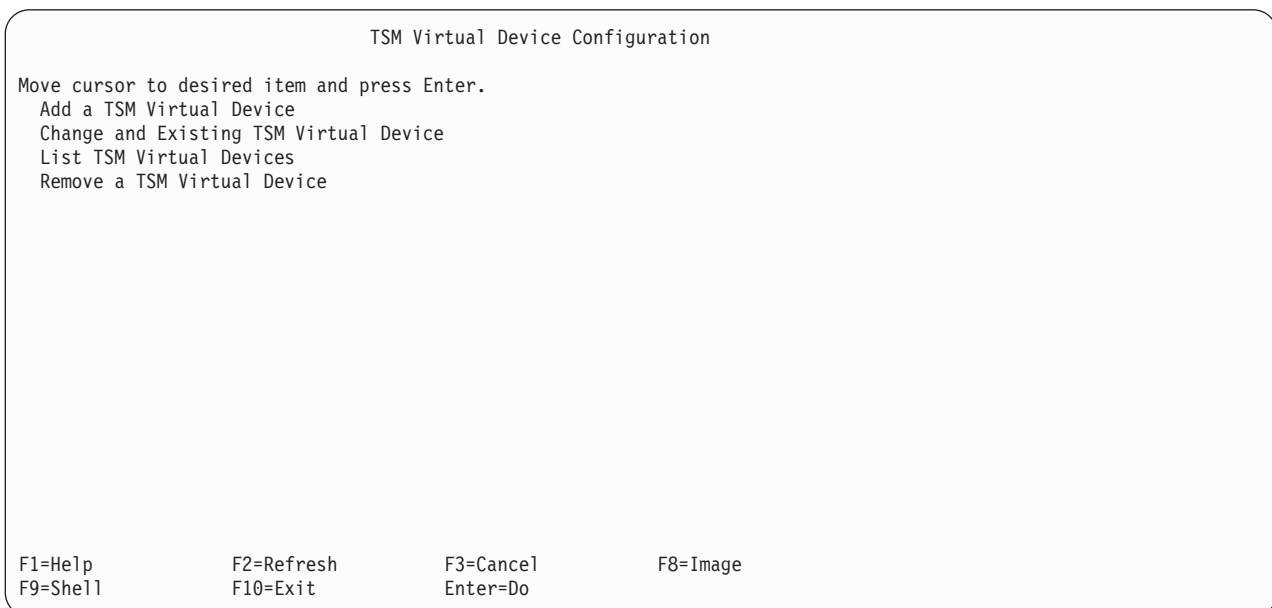


Figure 15-7. The TSM Virtual Device Configuration Menu

5. Select **Change an Existing TSM Virtual Device** and press Enter.
6. Highlight the desired virtual device to edit at the **Select a TSM Virtual Device** dialog and press Enter.

The following screen is displayed:

CHange an Existing TSM Virtual Device

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

TSM Virtual Device Name

TSM Server Name

Client Node Password

[Entry Fields]

tsm0

[lasher1_main]

+

F1=Help

F2=Refresh

F3=Cancel

F4=List

F5=Reset

F6=Command

F7=Edit

F8=Image

F9=Shell

F10=Exit

Enter=Do

Figure 15-8. The Change an Existing TSM Virtual Device Menu

7. Change the TSM server name listed in the **TSM Server Name** field if desired.

Note: The list of TSM server name stanzas is generated from the contents of the `/usr/tivoli/tsm/client/api/bin/dsm.sys` file.

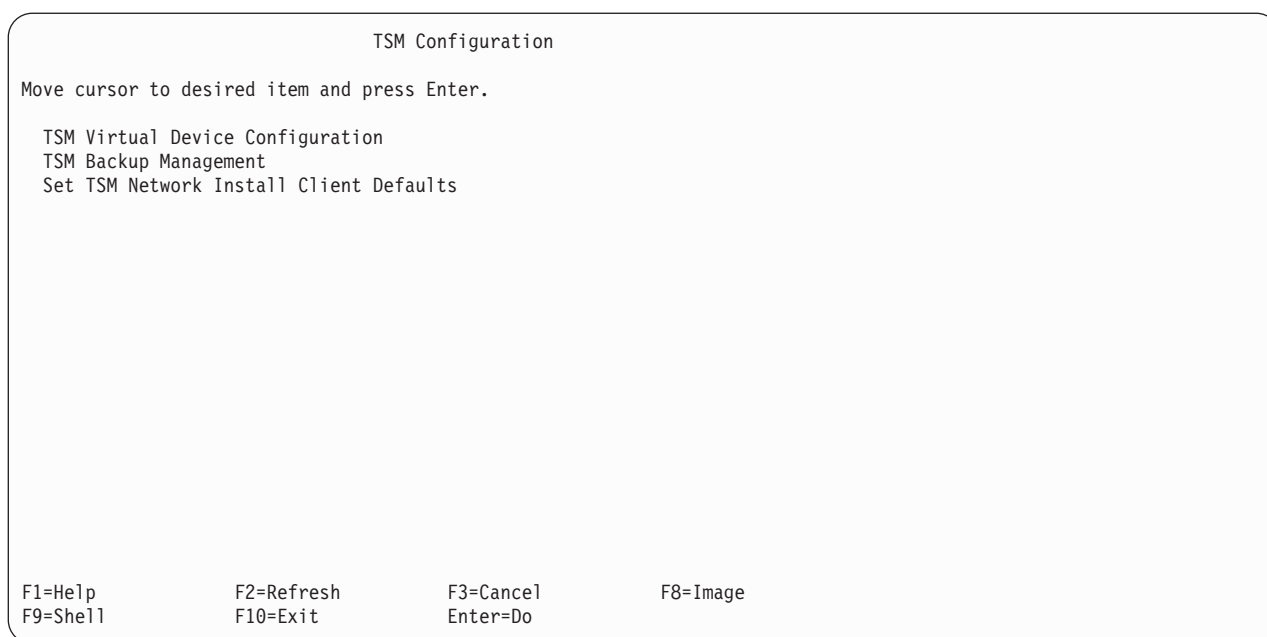
8. Enter the password for the client node name in the **Client Node Password**.
9. Press Enter.

Removing the TSM Virtual Device

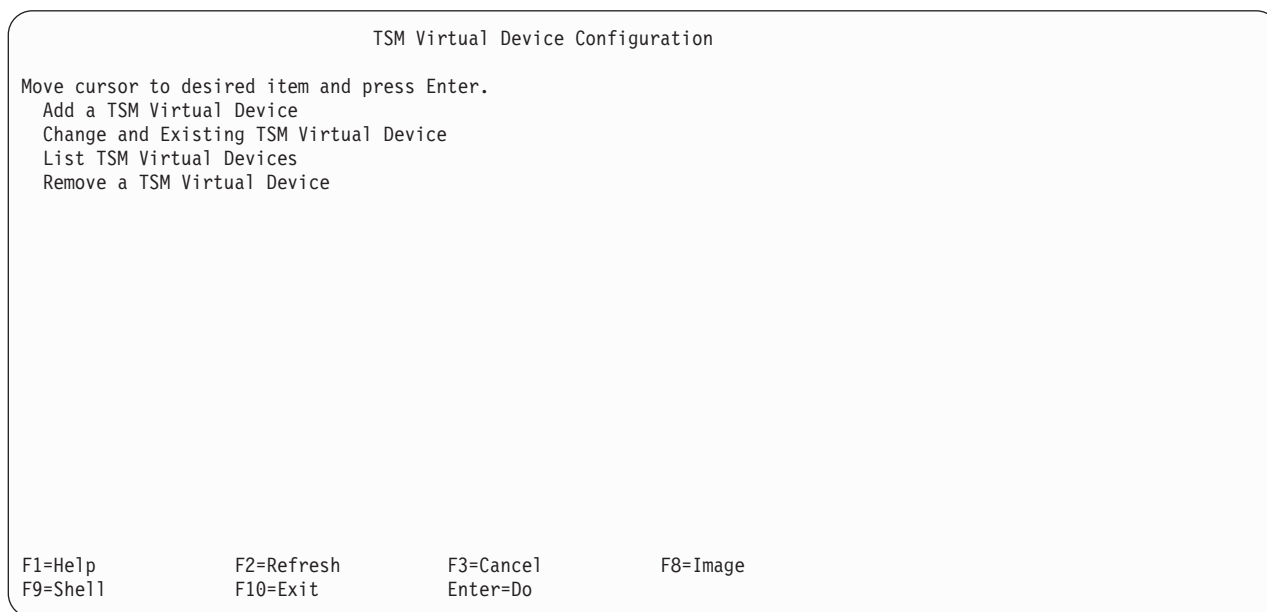
To access the TSM Virtual Device configuration menus:

1. Log in as the root user.
2. Type **smitty sysback** and press Enter.
3. Select **TSM Configuration** and press Enter.

The following screen is displayed:



4. Select **TSM Virtual Device Configuration** and press Enter.
The following screen will display:



5. Select **Remove a TSM Virtual Device** and press Enter.
6. Highlight the desired virtual device to remove from the **Select a TSM Virtual Device** dialog and press Enter.

Performing Backups to a TSM Server

Initiating backups to a TSM server is just like performing any other SysBack backup. Backup operations are initiated by the standard backup commands. However, rather than specifying a directory, tape, or CD / DVD drive as the backup device, the TSM virtual device is specified. Some backup command options are not valid when used for backups to a TSM server. If specified, a warning message will be issued and the invalid option will be ignored. For additional information regarding SysBack backups, please refer to Chapter 4, “Performing Backups”, on page 4-1 and to Appendix A, “Commands”, on page A-1.

Note: Each image that comprises a SysBack backup is sent to the TSM server as a single transaction. Therefore, TSM tuning options specific to client transactions are not applicable to this type of backup.

When setting up an exclude list for a backup using a TSM virtual device, it is important to remember that exclude lists must be defined from within SysBack since SysBack backup commands are executing the process. Exclude statements placed in the dsm.sys file, or in a TSM include / exclude file are not processed by the SysBack backup commands. For additional information regarding SysBack exclude lists, please refer to Chapter 9, “Exclude Lists”, on page 9-1.

Listing and Verifying Backups in a TSM Server

The list and verify functions within SysBack remain unchanged in regard to backups stored in a TSM server. The list option will attempt to read the table of contents file for the selected backup, where as, the verify option will attempt to read the actual backup image(s). However, rather than specifying a directory, tape, or CD / DVD drive as the backup device, the TSM virtual device is specified. For more information regarding listing and verifying backups, please refer to Chapter 18, “Listing or Verifying Backups”, on page 18-1.

Querying Backups and TSM Management Classes

Querying Backups

You may query information about the SysBack backup objects stored in a TSM server.

To list the backup objects stored in a TSM server:

1. Log in as the root user.
2. Type **smitty sysback** and press Enter.
3. Select **TSM Configuration** and press Enter.

The following screen is displayed:

```

TSM Configuration

Move cursor to desired item and press Enter.

TSM Virtual Device Configuration
TSM Backup Management
Set TSM Network Install Client Defaults


F1=Help      F2=Refresh   F3=Cancel    F8=Image
F9=Shell     F10=Exit    Enter=Do

```

Query TSM Backup Images

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

	[Entry Fields]	
TSM Virtual Device Name	tsm0	+
List Option	All	+
Backup Type	All	+
TSM Backup Image ID	[]	

F1=Help
F5=Reset
F9=Shell

F2=Refresh
F6=Command
F10=Exit

F3=Cancel
F7=Edit
Enter=Do

F4=List
F8=Image

Figure 15-13. The Query TSM Backup Images Menu

The fields have the following definitions:

TSM Virtual Device (Required)

Specify the virtual device that represents the connection information for the TSM server as configured in the `/usr/tivoli/tsm/client/api/bin/dsm.sys` file.

Note: The value for this field was populated from the entry made in the previous dialog prompt. However, this value may be changed from this screen as well.

List Option (Optional)

Specify the state of the backups that you would like to query. The default is "ALL". The available options are:

Active Active backup versions are the most recent copy of a backup type stored in the TSM server. There can be only one active version per backup type.

Note: For more information on active and inactive backup versioning, please refer to the *IBM Tivoli Storage Manager for AIX: Administrator's Guide* (GC32-0768).

Open Open backups represent currently running backup processes, or partial backup images created by an abnormally terminated backup process.

Note: Open backups listed that do not correspond to an actively running backup process should be removed to avoid versioning once the next backup process for that backup type is initiated.

All This option will list all active, inactive, and open backups for the backup type specified.

Note: Inactive backup versions are backups that are not the most recent backup for that backup type. There may be multiple

inactive versions for each backup type. The number of inactive versions is determined by the backup copy group defined on the TSM server. For more information regarding active and inactive backup versioning, please refer to the *IBM Tivoli Storage Manager for AIX: Administrator's Guide* (GC32-0768). For more information related to backup copy groups, please refer to the *IBM Tivoli Storage Manager for AIX: Administrator's Guide* (GC32-0768) and the *IBM Tivoli Storage Manager for AIX: Administrator's Reference* (GC32-0769).

This option is ignored when the **TSM Backup Image ID** is specified and required when specifying **Backup Type**.

Backup Type (Optional)

Specify the type of backup that you would like to query. The default is "ALL". The available options are:

System

Specify this option to display only Full System (Installation Image) backups.

Volume Group

Specify this option to display only Volume Group level backups.

File System

Specify this option display only File System level backups.

Logical Volume

Specify this option display only Logical Volume level backups.

File / Directory

Specify this option to display only File / Directory level backups.

ALL Specify this option to display all backup types.

This option is ignored when the **TSM Backup Image ID** is specified and required when specifying **List Option**

TSM Backup Image ID (Optional)

Specify the unique object id for the backup stored in the TSM server. When specifying this option, the **List Option** and **Backup Type** are ignored.

The output result when using the **List Option** and **Backup Type** will look similar to the following:

Backup ID	Type	Active?	Open?	Management Class	Backup Date
0.9527	FD	Yes	No	DEFAULT	02/14/2003 10:01:09

Note: The possible values for the **Type** field are:

- SB: Full System (Installation Image) backup
- VG: Volume Group level backup
- FS: File System level backup
- LV: Logical Volume level backup
- FD: File / Directory level backup

The output result when using the **Backup Image ID** option will look similar to the following:

Name	Size (MB)
/T0C	5
/hd4	7
/lv11	2
/hd3	2
/hd9var	4
/sblv	4

Querying Current Management Class Bindings

You may query the current management class bindings from within SysBack. The management class bindings are obtained from the server name stanza in the **dsm.sys** file that is associated with the specified TSM virtual device. If no bindings are specified, the value “default” is returned.

Note: SysBack automatically creates the necessary **dsm.opt** file when the TSM virtual device is created. It will be named **/usr/lpp/sysback/tsm/dsm.opt.tsmX** where X represents the TSM virtual device number.

To determine the current management class bindings:

1. Log in as the root user.
2. Type **smitty sysback** and press Enter.
3. Select **TSM Configuration** and press Enter.

The following screen is displayed:

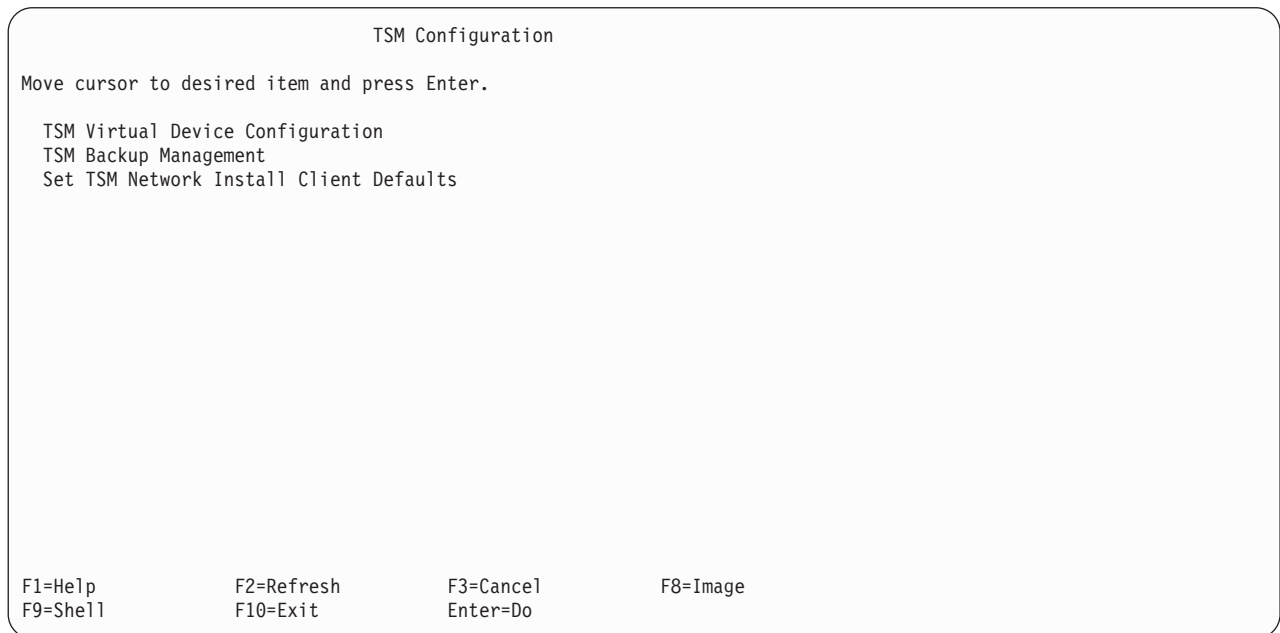


Figure 15-14. The TSM Configuration Menu

4. Select **TSM Backup Management** and press Enter.

The following screen is displayed:

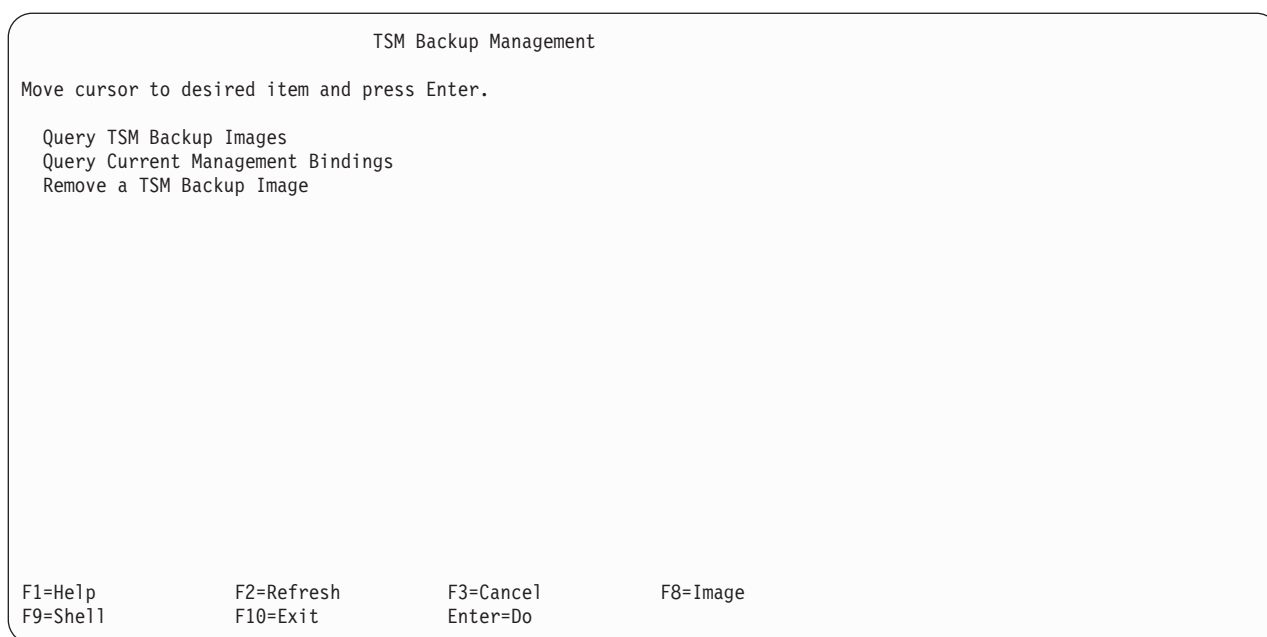


Figure 15-15. The TSM Backup Management Menu

5. Select **Query Current Management Bindings** and press Enter.
6. Highlight the virtual device to query at the **Select a TSM Virtual Device** dialog and press Enter.

The resulting output will look similar to the following:

```

                                COMMAND STATUS
Command: OK                      stdout: yes      stderr: no
Before command completion, additional instructions may appear below.
Backup Type   Management Class
-----
SB            DEFAULT
VG            DEFAULT
LV            DEFAULT
FS            DEFAULT
FD            DEFAULT

```

Note: The possible values for the **Type** field are:

- SB: Full System (Installation Image) backup
- VG: Volume Group level backup
- FS: File System level backup
- LV: Logical Volume level backup
- FD: File / Directory level backup

Querying File Spaces on the TSM Server

To determine or review the file space information related to backups with SysBack, issue the command

```
tsm> query filespace nodename *
```

from a TSM administrative command prompt.

Be aware that using the same TSM node name for both the TSM Backup / Archive Client client and the SysBack backup client will show different file space results than if they were separate. Please see the example below.

```
tsm> query filespace Num      Last Incr Date      Type
File Space Name ---      -----
----- 1      00/00/00  00:00:00  API:TSMVFS
/TSM4SBR 2      00/00/00  00:00:00  JFS
/home/tempvg2fs1
```

All backups created with SysBack will have a file space type of API:TSMVFS and a file space name of /TSM4SBR. SysBack However, backups created using the TSM Backup / Archive Client will have a file space type denoted by type of file system where the backup data resided, and the file space name will be the root of that file system or virtual mount point name.

Binding and Rebinding Backups to TSM Management Classes

Binding Backups

Binding is a TSM term that refers to associating a file with a management class. When a backup is performed, the backup objects (images) are either bound to the default management class for the active policy set, or the objects are bound to the management class specified in your include / exclude list.

Include statements are used to bind an object to a management class other than the default management class. The include statements are either placed directly in the **/usr/tivoli/tsm/client/api/bin/dsm.sys** file or into an include / exclude file referenced by the specified server stanza in the **dsm.sys** file.

Include statements to bind SysBack backups to a non-default management class are a little different than the usual TSM include statements. There are only 5 possible include statements that affect the binding of backups initiated by Sysback.

They are:

```
INCLUDE /TSM4SBR/SB/* FullSystemBackupClass
```

```
INCLUDE /TSM4SBR/VG/* VolumeGroupBackupClass
```

```
INCLUDE /TSM4SBR/LV/* LogicalVolumeBackupClass
```

```
INCLUDE /TSM4SBR/FS/* FilesystemBackupClass
```

```
INCLUDE /TSM4SBR/FD/* FileDirectoryBackupClass
```

These include statements bind an entire backup type to a management class. For example, the Full System Backup is comprised of a table of contents image and several logical volumes images that represent the data of raw logical volumes and / or logical volumes that have mounted file systems. Each and every image created by a single backup operation, whether it be 5 or 20 images, will be bound to the same management class. Backup images are grouped by TSM so that all components of a single backup operation will expire at the same time based on the management class attributes.

Rebinding Backups

Rebinding is a TSM term that refers to reassigning a backup to a different management class. When a backup type is rebound to a different management class, only the currently active backup, and all future backup operations after the management class is changed, will be rebound.

For example, let us assume that you performed full system backups on Monday, Tuesday, and Wednesday using the default management class. Then, on Thursday you assigned a new management class to the full system backup using an include statement. When the Thursday backup is initiated, the Thursday backup *and* the Wednesday backup will be rebound to the new management class.

Excluding Objects from Backups

In order to exclude specified files, directories, logical volumes, or file systems from backup processing, you must create an exclude list. The exclude list is created from within SysBack. TSM exclude statements located in a **dsm.sys** file will not be processed by SysBack backup commands. For more information regarding SysBack exclude lists, please refer to Chapter 9, “Exclude Lists”, on page 9-1.

Restoring Backups from a TSM Server

Initiating restore operations from a TSM server is just like performing any other SysBack restore. Restore operations are initiated by the usual restore commands. However, rather than specifying a directory, tape, or CD / DVD drive as the restore device, the TSM virtual device is specified. You must also specify the unique backup id associated for the backup object that you would like to restore. When performing a restore operation from within the SMIT interface, you will be presented with a selection list that looks similar to the following:

Backup ID	Type	Active?	Open?	Management Class	Backup Date
-----	----	-----	-----	-----	-----
0.6684	FD	No	No	DEFAULT	02/18/2003 13:07:
0.6686	FD	Yes	No	DEFAULT	02/18/2003 13:08:
0.6679	LV	Yes	No	DEFAULT	02/18/2003 13:06:
0.6659	SB	Yes	No	DEFAULT	02/17/2003 14:54:
0.6673	VG	Yes	No	DEFAULT	02/17/2003 15:31:
0.6636	FS	Yes	No	DEFAULT	02/17/2003 13:53:

Note: The output is displayed by descending date regardless of backup type. Within a date, the backups are grouped by type, and then by ascending time stamp for each type.

For additional information regarding SysBack restore operations, please refer to Chapter 10, “Recreating or Restoring from Backups”, on page 10-1.

Configuring Network Boot Options for a TSM Bare Metal Recovery

In order to perform a TSM bare metal recovery, the install client must initiate a network boot in order to access the SysBack **System Installation & Maintenance Main Menu**. For more information regarding the Installation and Maintenance menus, please refer to Chapter 12, “System Installation and Maintenance”, on page 12-1and to “Bare Metal Recovery and System Reinstallation from a TSM Server” on page 15-21.

Network boot configuration procedures are performed like any other SysBack network boot configuration. All of the same requirements apply with the following additional requirements:

- When performing a SysBack Classic Network Boot, the TSM 32-bit API client and the **tivoli.tivguid** (prerequisite of the API client) filesets must be installed on to the network boot server.
- When performing a SysBack NIM Resource Network Boot, the TSM 32-bit API client and **tivoli.tivguid** (prerequisite of the API client) filesets must be installed in to the NIM SPOT.

Note: There is not a SysBack utility available for installing the TSM filesets into the NIM SPOT. You must install them yourself using standard NIM commands.

For more information related to network boot configuration, please refer to Chapter 13, “Network Boot/Installation Configuration”, on page 13-1.

Optionally, you may choose to pre configure the **TSM Network Install Client Defaults** to avoid the manual entry of these values in the SysBack **Installation & Maintenance Main Menus**.

Note: You must configure the SysBack Network Boot Client for this system before setting this install defaults.

To access the TSM Network Install Client Default Menu:

1. Log in as the root user.
2. Type **smitty sysback** and press Enter.
3. Select **TSM Configuration** and press Enter.

The following screen is displayed:

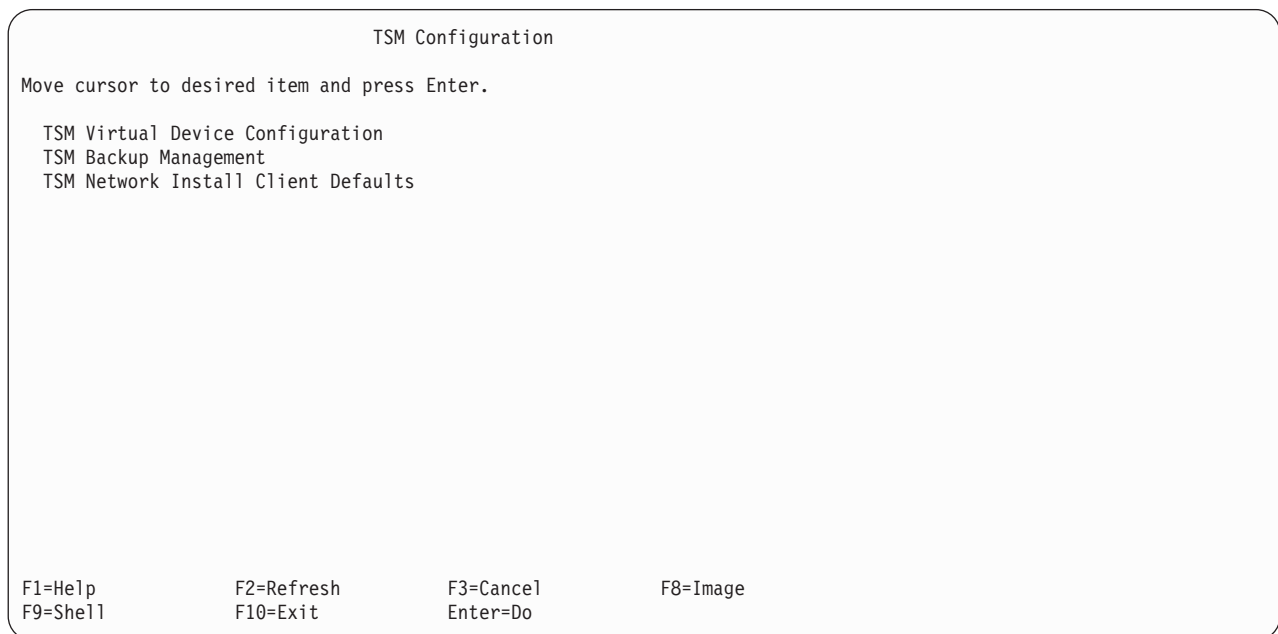


Figure 15-16. The TSM Configuration Menu

4. Select **TSM Network Install Client Defaults** and press Enter.
5. Highlight the desired network boot client when prompted in the **Select a Client Name** dialog and press Enter.

Note: The SysBack network boot client definition is based on the hostname of the client system. This may, or may not be, the same as the TSM client node name.

The following screen is displayed:

Set TSM Network Install Client Defaults

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

	[Entry Fields]
*Hostname	sysback2.aix.dfw.ibm.c>
TSM Client Node Name	<input type="text"/>
TSM Admin ID	<input type="text"/>
TSM Server Port	<input type="text"/>
Gateway	<input type="text"/>
Client Node or Admin Password	<input type="text"/>
TSM network device name	<input type="text"/> +
TSM Server IP address	<input type="text"/>
Subnet Mask	<input type="text"/>
Token-ring speed (if applicable)	<input type="text"/> +
Ethernet Interface (if applicable)	<input type="text"/> +
Ethernet Connection Type (if applicable)	<input type="text"/> +

Figure 15-17. The Set TSM Network Install Client Defaults Menu

6. Enter values for all applicable fields. The fields have the following definitions:

Hostname (Required)

Specify the hostname of the system which was configured as a SysBack network boot client. The value for this field was populated by the input in the previous menu.

Note: The SysBack network boot client definition is based on the hostname of the client system. This may, or may not be, the same as the TSM client node name.

TSM Client Node Name (Required)

Specify the TSM node name that will be used to connect to the TSM server for bare metal recovery.

TSM Admin ID (Optional)

Specify a TSM Admin ID that has client owner authority when the client node's password is unknown. When specifying a value in the field, you must also specify the Admin's password in the **Password** field rather than the client node password.

TSM Server Port

Specify the TSM server port number that should be used to connect to the TSM server for bare metal recovery.

Gateway

Specify the gateway address that this client system must go through in order to access the server system. If the client and the server are on the same subnet, it is recommended to re-enter the server's IP address here.

Client Node or Admin Password

Specify the TSM client password that is associated with the **TSM Client Node Name** value. If you do not know the password of the client node name, enter the password to administrative id created for this node

which has client owner authority. In most cases, this was automatically created when you registered the node to the TSM server.

Note: If you do not know either password, you will have to log on to the TSM server as an administrator and issue the command: **update node your_nodename new_password**. Then enter that new password into this field.

TSM Network Device Name

Specify the network device name to use for communications with the TSM server. For example: ent0.

TSM Server IP Address

Specify the IP address that corresponds to the TCPServeraddress for the TSM server as defined in the file `/usr/tivoli/tsmserv/bin/dsmserv.opt` on the TSM server system.

Subnet Mask

Specify the subnet mask, if required, for the client network interface to contact the installation server.

Token-ring Speed (if applicable)

Specify the correct token-ring speed when a token-ring device specified in the **TSM Network Device** field.

Ethernet Interface (if applicable)

Specify either type of ethernet interface when an ethernet device is specified in the **TSM Network Device Name** field. For example: IEEE 802.3

Ethernet Connection Type (if applicable)

Specify the connection type for the ethernet interface when an ethernet device is specified in the **TSM Network Device Name** field. For example: BNC.

7. Press Enter to set the defaults.

For more information regarding the registration of a TSM node or determining the correct TSM Server port to use, please refer to the *IBM Tivoli Storage Manager for AIX: Administrator's Guide (GC32-0768)* and the *IBM Tivoli Storage Manager for AIX: Administrator's Reference (GC32-0769)*.

Bare Metal Recovery and System Reinstallation from a TSM Server

Performing a system installation, or bare metal recovery, using a backup stored in a TSM server is just like any other SysBack system installation with the following exceptions:

- You must network boot the system to the **Installation and Maintenance Main Menu**. Tape, CD, or DVD device boots are not supported.
- The installation device will be a TSM virtual device rather than a tape, CD, DVD, or another network install server.

Once you have successfully executed a network boot, the following menu will be displayed:

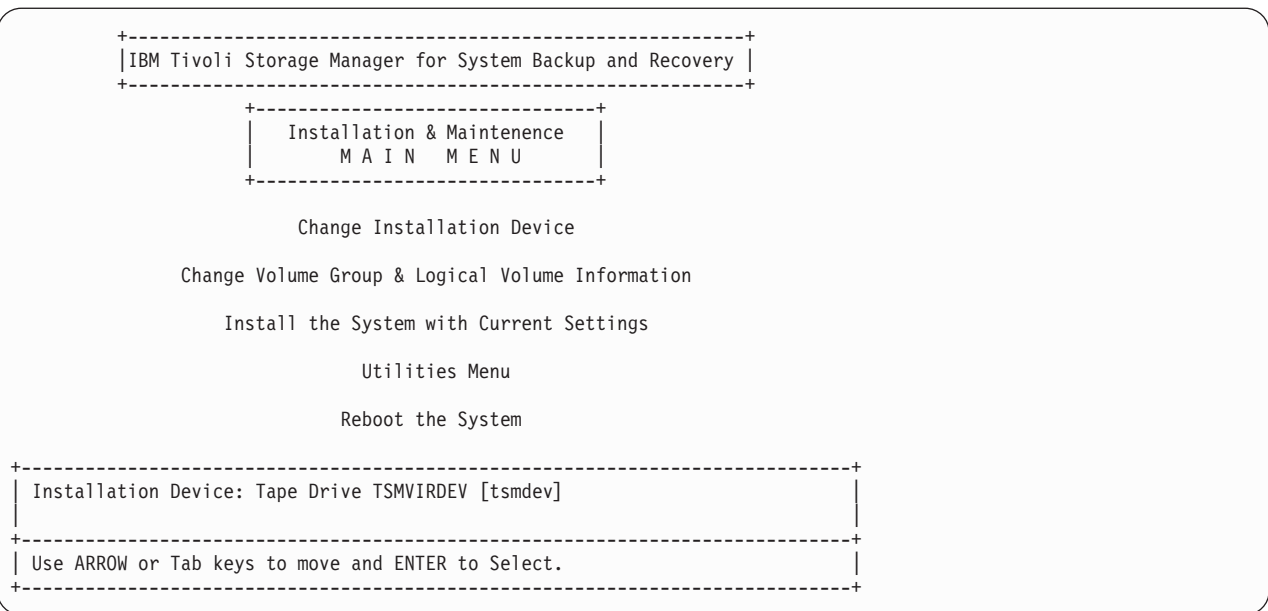


Figure 15-18. The SysBack Installation and Maintenance Menu

To verify or change the network information required to connect to a TSM server for retrieval of the SysBack backup image, select **Change Installation Device** to display the following menu:

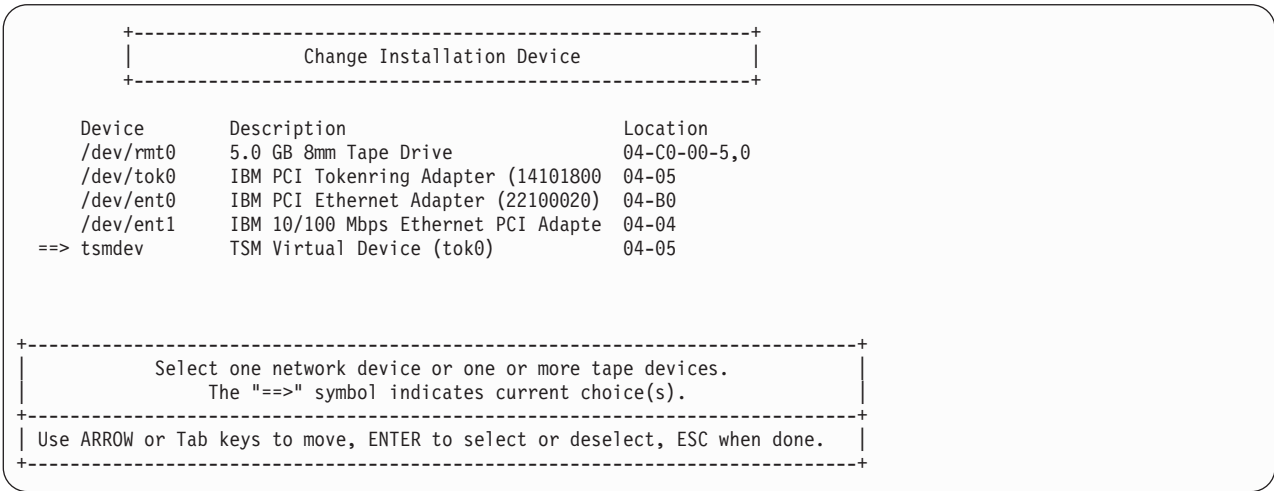


Figure 15-19. The Change Installation Device Menu

Select the tsmdev device to verify or change the network interface associated with this restore process. The following menu will be displayed:

```

+-----+
|               Change Network Interface               |
+-----+

Device      Description                               Location
==>/dev/tok0  IBM PCI Tokenring Adapter (14101800)  04-05
/dev/ent0    IBM PCI Ethernet Adapter (22100020)  04-B0
/dev/ent1    IBM 10/100 Mbps Ethernet PCI Adapte  04-04

+-----+
|               Select one network device or one or more tape devices.               |
|               The "==" symbol indicates current choice(s).                         |
+-----+
| Use ARROW or Tab keys to move, ENTER to select or deselect, ESC when done.       |
+-----+

```

Figure 15-20. The Change Network Interface Menu

Select the desired network interface and press Enter to verify or change the network settings associated with this restore process. The following screen will be displayed:

```

+-----+
|               Change TSM Network Settings               |
+-----+

Client IP Address      192.168.1.58
Client Node Name       lasher
TSM Admin ID
Server IP Address      192.168.1.55
Gateway IP Address     192.168.1.58
Subnet Mask            255.255.255.192
Port Number            1500
Password:              tsmpass
Token-ring Speed:
    4 megabits
    ==> 16 megabits
Network Adapter: tok0 [inactive]

+-----+
| Enter the TSM server port number that corresponds to the desired TSM server      |
| connection for this installation.                                                |
+-----+
| Use ARROWS or Tab to move or INS/DEL to edit. Press ESC to return.             |
+-----+

```

Figure 15-21. The Change TSM Network Settings Menu

Verify or edit the values in each field as required for this restore process. The fields have the following definitions:

Client IP Address (Required)

Specify the IP address of this client system. Do not enter leading zeros in the address.

Client Node Name (Required)

Specify the TSM client nodename that was used to create the backup object that you would like to restore. This may, or may not be, the same name as the hostname returned by the **Client IP Address** specified above.

TSM Admin ID (Optional)

Specify a TSM Admin ID that has client owner authority when the client node's password is unknown. When specifying a value in the field, you must also specify the Admin's password in the **Password** field rather than the client node password.

Server IP Address (Required)

Specify the IP address of the server system that will be used to reinstall this client. This should be the system running the TSM server that has the desired backup object to restore. If the boot server is the same as the installation server, do not change this value unless you have chosen a different network interface to perform the installation. If you are choosing a different network interface to perform the install, or the installation server is different than the boot server, enter the correct address. Do not enter leading zeros in the address.

Gateway IP Address (Optional)

Specify the gateway address that this client system must go through in order to access the server system. If the client and the server are on the same subnet, it is recommended to re-enter the server's IP address here.

Subnet Mask (Optional)

Specify the subnet mask, if required, for the client network interface to contact the installation server.

Port Number (Required)

Specify the port number that accepts client connections as defined on the TSM server. If you do not know the port number defined for the TSM server, you must check the `/usr/tivoli/tsm/server/bin/dsmserv.opt` file located on the TSM server system.

Password (Required)

Specify the TSM client password that is associated with the **Client Node Name** value. If you do not know the password of the client node name, enter the password to administrative id created for this node which has client owner authority. In most cases, this was automatically created when you registered the node to the TSM server.

Note: If you do not know either password, you will have to log on to the TSM server as an administrator and issue the command: **update node your_nodename new_password**. Then enter that new password into this field.

Token-ring Speed

Specify the correct token-ring speed when a token-ring device specified as the network adapter.

Ethernet Interface (if applicable)

Specify either type of ethernet interface when an ethernet device is specified as the network adapter. For example: IEEE 802.3

Ethernet Connection Type (if applicable)

Specify the connection type for the ethernet interface when an ethernet adapter is specified. For example: BNC.

Once you have configured the installation device settings as desired, you will need to query the TSM server and select the backup object to restore. The easiest way to achieve this is to access the **Change Volume Group & Logical Volume Information** menu. Selecting this menu after setting your tsmdev installation device settings will cause SysBack to query the correct TSM server to obtain a list of backup objects available for restore.

Tivoli Storage Manage for System Backup and Recovery			
Backup ID	Ative	Management Class	Backup Date
=> 0.1345	Yes	SystemBackupClass	01/19/03 11:56:00
0.1214	No	SystemBackupClass	01/18/03 13:10:05
0.1010	No	OldBackupClass	01/15/03 09:54:25
Select the ibackup ID to use from the above list The "=" symbol indicates current choice(s).			
Use ARROW or Tab keys to move, ENTER to select or deselect, ESC when done.			

Figure 15-22. The Backup Image to Restore Selection Menu

Once you have selected the backup object to restore, you are ready to customize any other installation attributes as desired. If you do not need to make any changes, simply begin the install.

Additional Information Resources

For more information related to network boot, please refer to Chapter 13, "Network Boot/Installation Configuration", on page 13-1.

For more information related to the network boot of SP systems, please refer to Chapter 14, "RS/6000 Scalable POWERParallel Systems® (SP) Boot and Install Utilities", on page 14-1.

For more information related to the system installation process using SysBack, please refer to Chapter 12, "System Installation and Maintenance", on page 12-1.

For examples of how to physically boot various RS/6000 or pSeries systems, please refer to Appendix B, "Booting a System for SysBack Installation or Maintenance", on page B-1 or review the hardware reference manual for your particular RS/6000 or pSeries system.

For examples related to reinstalling LPAR Capable systems, please refer to the IBM Redbook *The Complete Partitioning Guide for IBM @server pSeries Servers*, SG24-7039-00 located at <http://www.redbooks.ibm.com/pubs/pdfs/redbooks/sg247039.pdf>

Using Multiple Backup and Restore Sessions

You may initiate multiple backup and / or restore sessions using a TSM virtual device provided that each session is for a unique backup type. For example, you may perform a volume group level backup and a file system level backup concurrently. However, you may not perform two volume group backups concurrently.

Failure to adhere to this limitation could result in unpredictable, undesirable results and will not be supported.

Problem Determination

Understanding basic SysBack and TSM problem determination tools may help you resolve minor problems without the need to contact support. In those situations where you would like to contact support for assistance, understanding the tools that support may ask you to use may be helpful as well.

There are 3 primary items that you should monitor or review periodically to ensure that all of your backup processes are functioning properly. They are:

- The SysBack command output
- The SysBack Activity Log
- The SysBack error log for the TSM API

The SysBack Command Output

The most effective way to ensure that your backup operations are completing without error is to save the output from the backup operation. Sometimes, a backup completes with a status of success but also had warning messages. In order to determine what exactly caused the warning, you will need to look at the output from the command. There have been scenarios where an overall backup process completed successfully, but due to an unforeseen operating system issue, much of the data was not actually backed up.

In order to capture the output of the SysBack backup operations, you must redirect standard output and standard error to a file.

This may be achieved by issuing your command in a manner like this:

```
/usr/sbin/sysback -f tsm0 datavg > /tmp/backup.log 2>&1
```

If you would like to monitor the backup process on your screen and save the output to a file at the same time, you could issue a command like this:

```
/usr/sbin/sysback -f tsm0 datavg 2>&1 | tee /tmp/backup.log
```

There are several different methods for capturing the standard output (stdout) and standard error (stderr) from a command. There are also several ways to rotate your backup logs or to dynamically created the log name. Simply choose the method that is appropriate to your environment.

The SysBack Activity Log

SysBack provides a basic Activity Log that indicates the start date and time of all backup, restore and verify operations. It also includes the command issued, and if the command was successful, failed, and / or had warnings.

For more information regarding the SysBack Activity Log, please refer to: Chapter 19, “Activity Logging”, on page 19-1.

SysBack Error Log for the TSM API

The TSM API error log specific to the SysBack initiated communications is located at **/usr/lpp/sysback/sbtsmerror.log**. You should periodically review this file for issues related to TSM server communications.

Note: You can override this location by setting the **DSMI_LOG** environment variable in your **.profile** or **.kshrc** file.

Debug Options

Occasionally, more detailed information is needed for diagnosis, these 4 primary options are available:

- Putting the SysBack programs into debug
- Putting SysBack TSM API programs into debug
- Tracing the TSM API programs
- Putting the installation process into debug

Please contact support for detailed information with using any of these debug options.

Interoperability with System Backup and Recovery for AIX - SysBack Versions 5.1 - 5.4

IBM Tivoli Storage Manager versions 5.5 or 5.6 backups created to backup media other than the TSM virtual device may be restored by System Backup and Recovery for AIX - SysBack versions 5.1 - 5.4.

Likewise, backups created by System Backup and Recovery for AIX - SysBack versions 5.1 - 5.4 may be restored using non-TSM devices with IBM Tivoli Storage Manager versions 5.5 and 5.6.

Chapter 16. Utilities

The utilities menu contains options for performing special tasks, usually those used by advanced users or that are performed only periodically.

To access the utilities menu:

1. At a command line, type `smit`.
2. From the SMIT menu, select **IBM Tivoli Storage Manager for System Backup and Recovery**.
3. Select **Utilities**.

The Utilities menu is shown below. These options change more frequently than other SysBack options, because new utilities are introduced into SysBack more often than other functions. Also, items are removed as they become obsolete or are integrated with other features of the system.

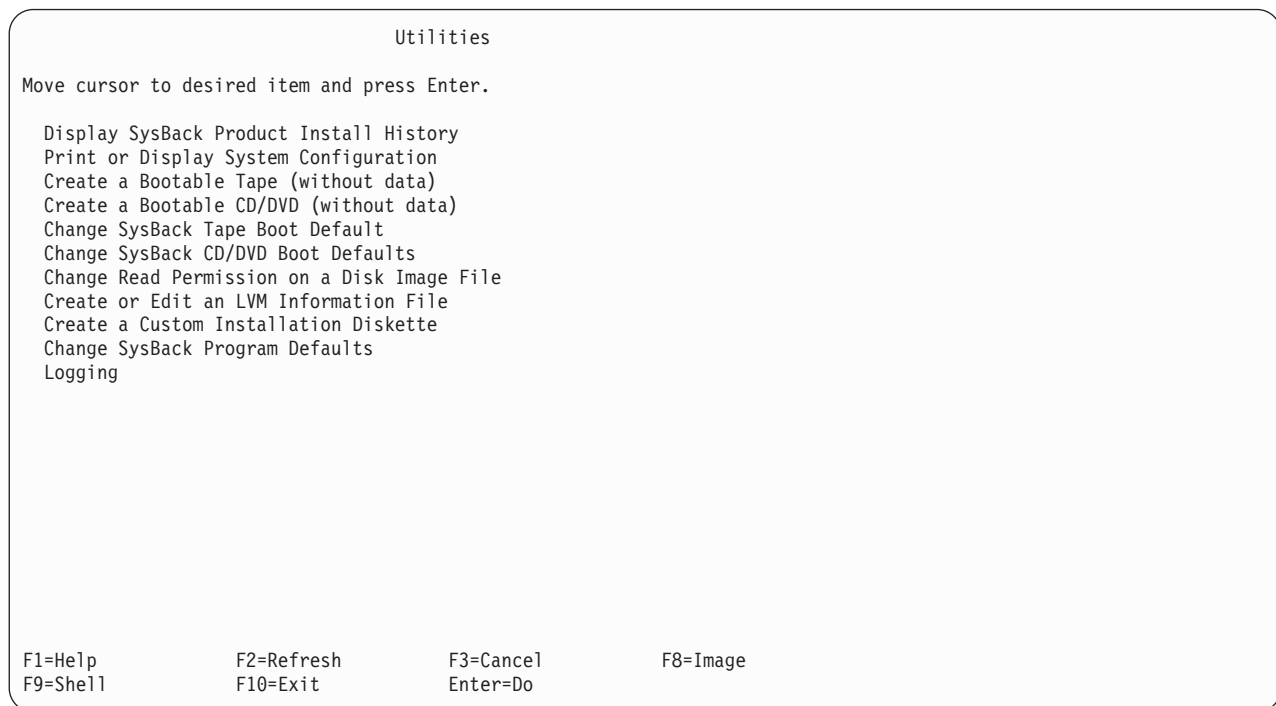


Figure 16-1. The Utilities Menu

The options available on the Utilities menu are described in the following sections.

Displaying SysBack Product Installation History

You might want to know the installation history of SysBack, particularly when deciding if product updates are required. Using the **Display SysBack Product Install History** option, you can create a list containing the dates and levels of the initial SysBack installation and any product updates to date. The list contains the main SysBack product, as well as, any additional product features that are installed separately.

To display the product history, select **Display SysBack Product Install History** from the Utilities menu. You can also create this list using the fastpath `smit sb_showlevel` at the command line.

Printing or Displaying System Configuration

Use the **Print or Display System Configuration** option to document the system configuration, including all information pertaining to the volume groups, physical volumes, logical volumes, and filesystems. It provides a report that contains all of the key information that you might need in case of various system failures.

In most cases, you do not need this information when recovering from system failures, because the SysBack installation process and the **remakevg** command recreates volume groups, logical volumes, and filesystems without requiring the user to have knowledge of the system configuration. This information, however, might be useful in planning a migration of filesystems to new hardware or in reorganizing an existing system to take advantage of disk striping, mirroring, or other features.

To print or display the system configuration:

1. Select **Print or Display System Configuration** from the Utilities menu.
2. The following options are displayed:

Enter print queue name ([]=display)

The default value is the current default printer as defined by either the `PRINTER` environment variable or the first print queue in the `/etc/qconfig` file. Enter the name of the print queue where you want to send the report or leave blank to display on the screen.

Enter filename to save ([]=display)

Default=blank. Enter the full pathname of the file where you want to save the report or leave blank to display on the screen.

Note: Both of the above fields must be blank to show the report on the screen.

3. Press Enter to print the report.

The report output includes the following information:

Volume group information

One record for each volume group. Contains all volume group attributes and physical volume sizes. Example:

Volume Group	Auto-on?	PP Size	Quorum?	Total	Used	Free	PV(s)
rootvg	y	4 MB	y	250 PPs 1002 MB	213 PPs 852 MB	37 PPs 148 MB	hdisk0

Logical Volume Information

One record for each logical volume. Contains most logical volume attributes and a list of the physical volumes each logical volume resides on. Example:

Volume Group	Logical Volume	Attributes			
rootvg	hd8	Type:	jfslog	Copies:	1
		LPs:	1	IntraPV:	c
		MinLps:	0	InterPV:	m
		PV(s):	hdisk0	Upper:	32
				StrpSz:	0

Physical Volume Information

One record for each physical volume. Contains the physical volume location, size and a map of the regions on the disk where each logical volume resides.

For example:

PV Name	Volume Group	Location	PVID	MB	PPs
hdisk0	rootvg	00-00-0S-0,0	00000218acd0f607	1002	250
	LV Name	PPs	Region		
	hd8	101X....		
	hd6	51-62	..X.....		
		73-96	..XX.....		
	hd4	3	X.....		
		102-103X....		
	hd3	105-109X....		
	hd2	5-27	XX.....		
		110-207XXXXX.		
		222-242X		

Filesystem information

All filesystem attributes. Note that the *BF Spt* and *AG Size* fields are displayed only on AIX 4.2 or later systems. Example:

Volume Group	Mount Point	FragSz	NBPI	Cmprs	BF Spt?	AG Size?
rootvg	/	4096	2048	no	n	8
	/home	512	4096	no	y	8
	/tmp	4096	4096	no	n	8
	/usr	4096	4096	no	n	8
	/var	512	4096	no	n	8
	/data/files	512	4096	no	y	32

Logical Volume Partition Maps

The specific physical partitions on the physical volumes that are used by each logical volume. This determines the fragmentation of logical volumes. Example:

Volume Group	Logical Volume	Copy#	PV Name	PP#s	PV Region
rootvg	hd8	1	hdisk0	101-101X....
	hd6	1	hdisk0	51-62	..X.....
		1	hdisk0	73-96	..XX.....
	hd4	1	hdisk0	3	X.....
		1	hdisk0	102-103X....
	hd3	1	hdisk0	105-109X....
	hd2	1	hdisk0	5-27	XX.....
		1	hdisk0	110-207XXXXX.
		1	hdisk0	222-242X

Creating a Bootable Tape (Without Data)

Use the **Create a Bootable Tape (without data)** option to create a bootable tape on the local system or a remote server. This bootable tape is identical to a system backup except that it does not contain any backup data.

The primary intention of this option is to enable you to create a tape that can be used to boot a system to the SysBack Installation and Maintenance Menus without having to perform a full backup. This tape enables the user to perform system maintenance or to boot from an alternate media if the boot images on a prior system backup tape are corrupt or do not contain updated device information.

You can also boot from a tape containing required device support software to perform a network installation from media on a remote server. In this case, you must explicitly indicate that the network support be included on the tape. When booting from tape to perform a network installation, the server on which the installation media is present does not need the device support installed to support the client, but the installation media itself must contain the required device support.

Cloning systems: A boot tape created on one machine can be used on another machine with a different processor or platform type. The system backup created on one machine can also be installed on another machine, even if the device configuration differs. When cloning systems, the machine on which the boot tape is created must have installed all of the device and system support software for the destination platform type, processor type, and other required devices.

To create a bootable tape:

1. From the Utilities menu, select **Create a Bootable Tape (without data)**.

Note: From the command line, type `smit sb_mkboottape`.

2. On the Device Selector screen, highlight the device you want to use and press Enter.
3. The following screen is displayed:

Create a Bootable Tape (without data)

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

	[Entry Fields]	
Device name	[/dev/rmt0]	/
Hostname of server		
Platform/kernel type for tape boot image	[rspc]	+
Network install support to include	[ent]	+

F1=Help

F5=Reset

F9=Shell

F2=Refresh

F6=Command

F10=Exit

F3=Cancel

F7=Edit

Enter=Do

F4=List

F8=Image

Figure 16-2. The Create a Bootable Tape (without data) Menu

The fields have the following meanings:

Hostname of server

The server hostname if a server option was selected on the prior device selector screen. You cannot change this field.

Device name

The device, if a tape drive or virtual device was selected. You cannot change this field from this screen.

Platform/kernel type for tape boot image

Default=current platform/kernel type. This field is displayed only

when you use a tape drive or virtual device. Change this field only if you are creating a backup that is to be installed (cloned) onto another platform type or to a machine running a different kernel. Press F4 to list the platforms/kernels for which tape boot support is installed on the system and select from the list.

The following platform/kernel types are currently supported:

chrp	Common Hardware Reference
chrp/MP	Multiprocessor Common Hardware Reference Platform
rs6k	RISC System/6000 (uniprocessor)
rs6k/MP	Multiprocessor RISC System/6000
rspc	PCI-based (PC) RISC System/6000 (uniprocessor)
rspc/MP	Multiprocessor PCI-based (PC) RISC System/6000

Network install support to include

Default=(Blank/None). If, after booting a system from this backup tape, you want to perform a network installation (rather than installation from this backup), press F4 to display a list of supported network types and select a network type from the list. You must select the network type of the adapter that will be used to install the system from the network server.

4. Press Enter to begin creation of the bootable tape.

Creating a Bootable CD/DVD (Without Data)

Use the **Create a Bootable CD/DVD (without data)** option to create a bootable CD or DVD on the local system or a remote server. This bootable media is identical to a system backup except that it does not contain any backup data.

The primary intention of this option is to enable you to create a CD or DVD that can be used to boot a system to the SysBack Installation and Maintenance Menus without having to perform a full backup. This media enables the user to perform system maintenance or to boot from an alternate media if the boot images on a prior system backup are corrupt or do not contain updated device information.

You can also boot from a CD or DVD containing required device support software to perform a network installation from media on a remote server. When booting from CD or DVD to perform a network installation, the server on which the installation media is present does not need the device support installed to support the client, but the installation media itself must contain the required device support.

Cloning systems: A boot CD or DVD created on one machine can be used on another machine with a different processor or platform type. The system backup created on one machine can also be installed on another machine, even if the device configuration differs. When cloning systems, the machine on which the boot media is created must have installed all of the device and system support software for the destination platform type, processor type, and other required devices.

To create a bootable CD or DVD:

1. From the Utilities menu, select **Create a Bootable CD/DVD (without data)**.

Note: From the command line, type `smit sb_mkbootcd`.

2. On the Device Selector screen, highlight the device you want to use and press Enter.
3. The following screen is displayed:

Create a Bootable CD/DVD (without data)

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

	[Entry Fields]	
Device name	[/dev/cd0]	/
Media Type?	DVD	
Media Size	<input type="text"/>	#
Platform type(s) for CD/DVD boot image	[chrp]	+
Create the CD/DVD Now?	yes	+
Debug Output?	no	+
HOST OPTIONS:		
Build Temp Work Space(s) on	N/A	+
Hostname of CD/DVD Server	<input type="text"/>	
SOFTWARE OPTIONS:		
Location of Software Packages to copy to CD/DVD.	<input type="text"/>	/
File with list of packages to copy to CD/DVD	<input type="text"/>	/
WORK SPACE OPTIONS:		
File system to store CD/DVD file structure	<input type="text"/>	/
File system to store final CD/DVD image	<input type="text"/>	/
Local Volume Group for creation of filesystems	<input type="text"/>	+
Remote Volume Group for creation of filesystems	<input type="text"/>	+
Do not remove the final CD images	<input type="text"/>	+

F1=Help
F2=Refresh
F3=Cancel
F4=List

F5=Reset
F6=Command
F7=Edit
F8=Image

F9=Shell
F10=Exit
Enter=Do

Figure 16-3. The Create a Bootable CD/DVD (without data) Menu

The fields have the following meanings:

Device Name

Specify CD / DVD device in the form of /dev/cd0.

Media Type?

Specify the device / media type. Valid options are CD and DVD.

Media Size

Specify the media size in MB to override default values. Default CD size is 650MB. Default DVD size is 4188 MB (4.09 GB). If the side of your media is double sided, only specify the size of one size of the media, not the total aggregate.

Platform type(s) for CD/DVD boot image

Specify the platform type of the system where the CD / DVD will be utilized. Select one or more options. If you are creating the CD / DVD on the system where it will be used to boot and install, it is not necessary to change this option as the process will default to the current platform type. For example: If you were creating this CD / DVD on an F50, it would be created to support the CHRP platform. If you are creating the CD / DVD to support this system and a second type of system, such as the default CHRP and also for an RSPC system, you would specify chrp rspc.

Note: The list of platform types must be space separated.

This option requires that all of the device and kernel support required to boot both platforms be installed onto the system creating the CD / DVD. Failure to have all of the needed support installed will not cause

the backup and CD / DVD creation to fail. Instead, it will cause the boot to fail when booting from a platform different than where the CD / DVD was created. Optionally using the **Location of Software Packages to copy to CD/DVD** field along with this option will allow you to place this device support for both platforms into the CD / DVD boot image and also allows it to be utilized as Post Install device support media. This would be useful when you want to boot from this CD / DVD which has all needed device support, but install from a backup (tape, CD, DVD, file) that does not have all of the needed support in the backup image. Entering **ALL** in this field creates a CD / DVD that may be used to boot any system and requires the use of the **Location of Software Packages to copy to CD/DVD** which provides all device support to be built into the boot images allowing this to be true. You will also be able to utilize this media as Post Install device support.

Note: Specifying this option will perform an `installp` command against the **Location of Software Packages to copy to CD/DVD** device or directory and installs those filesets onto this system. Also, this support is placed onto the CD / DVD for use as Post Install device fileset media.

Create the CD/DVD Now?

Stops the `/usr/sbin/mksbcd` command before writing to media without removing the final CD image. This leaves you with a final Rockridge Image that may be burned to CD / DVD at a later time. The backup_image file system and the cd_fs file system will be removed thereby will leave only the cd_image file system with the Rockridge Image (iso). If you select this option, you will have to manually burn the image to CD / DVD yourself using the GNU `burn_cd` function instead of using SysBack.

Debug Output?

Sets the environment variable `SBDEBUG=1` to enable debugging of SysBack programs.

Build Temp Workspace(s) on?

This field is based on if you chose a local or remote device in the device selector screen. If you selected a local device, this will be set to N/A. If you selected a device on a remote host, you have two options for determining where the work spaces will be created. The values are:

Server Specify this option to create the backup_image, cd_fs, and cd_image file systems on the remote system. You may optionally use the **Remote Volume Group for creation of filesystems** option to specify which volume group on the remote system in which the 3 file systems will be created.

Client Specify this option to create the backup_image, cd_fs, and cd_image file systems on the local system and the "cd_image" file system on the remote system. You may optionally use the **Local Volume Group for creation of filesystems** option to specify which volume group on the remote system in which to create the cd_image file system.

Hostname of CD/DVD Server

Specify the hostname of the remote system where the work space will be created. This option is only valid when **Build Temp Workspace(s) on?** is set to Server or Client.

Location of Software Packages to copy to CD/DVD.

Specify the device or directory containing AIX device and/or kernel support filesets in the bffcreate format for use in either creating boot images or for use as Post Install Device support. This flag is required with the **Platform type(s) for CD/DVD boot images** set to all, and optional with any other combination.

File with list of packages to copy to CD/DVD.

Specifies a file that contains a list of additional software packages that will be stored in the **/usr/sys/inst.images** subdirectory of the cd_fs file system. This option requires the use of the **Location of Software Packages to copy to CD/DVD** as these packages will be copied from that file system or device. This would be useful when there are AIX filesets that you would like to have installed, but are not considered required device or kernel support filesets. You may also store other third party software product that you would like to be automatically installed.

File system to store CD/DVD file structure

Specify the name of an existing file system to be used in place of the default cd_fs file system. You must ensure that there is enough space in this file system as outlined in the section entitled "Space" on page 5-2. If this option is not specified, the default cd_fs file system created is **/mksbcd/cd_fs**. If there is not enough space in this file system, the mksbcd command will enlarge the file system with the AIX **/usr/sbin/chfs** command to make it large enough. If the chfs command fails, then so will mksbcd. Also, this file system will not be automatically removed by the mksbcd command. However, it's contents will be removed unless you specify the **Do not remove the final CD images** option.

File system to store final CD/DVD image

Specify the name of an existing file system to be used in place of the default cd_image file system. You must ensure that there is enough space in this file system as outlined in the section entitled "Space" on page 5-2. If this option is not specified, the default cd_image file system created is **/mksbcd/cd_image**. If there is not enough space in this file system, the mksbcd command will enlarge the file system with the AIX **/usr/sbin/chfs** command to make it large enough. If the chfs command fails, then so will mksbcd. Also, this file system will not be automatically removed by the mksbcd command. However, it's contents will be removed unless you specify the **Do not remove the final CD images** option.

Local Volume Group for creation of filesystems

Specify this option when you do not want the default backup_image, cd_fs, and cd_image file systems created in the rootvg volume group. This only applies when the **Hostname of CD/DVD Server** option is used.

Remote Volume Group for creation of filesystems

Specify this option when you do not want the default backup_image, cd_fs, and cd_image file systems created in the rootvg volume group. This only applies when the **Hostname of CD/DVD Server** option is used.

Do not remove the final CD images

Specify this option when you do not want the mksbcd process to

remove one or more of the default created file systems. Specify one or more of the following combinations:

C Do not remove the cd_fs file system I Do not remove the cd_image file system

This value may be specified as CI or C I.

4. Press Enter to begin creation of the bootable CD or DVD.

Changing SysBack Tape Boot Defaults

Use the **Change SysBack Tape Boot Defaults** menu to set tape boot defaults. Setting tape defaults will let you minimize, possibly eliminate, user prompting during a tape boot or installation process. These defaults are stored in a file named **/sbin/install.data**. Therefore, you must set these options before the backup is executed, or boot only tape created, in order to ensure that this file is included in the boot image. It is the file that is used during the boot and installation process that processes these specifications.

This is similar to the **Set Network Install Client Defaults** menu for network boot or installation processes.

To set the Tape Boot Defaults:

1. From the Utilities menu, select **Change SysBack Tape Boot Defaults**.

Note: From a command line, type `smit sb_cfginsttape`.

2. The following screen is displayed:

Note: You may also access this same menu by using the following SMIT paths:

```
smitty sysback          Sysback Program Defaults
                        Change Sysback Program Defaults
                        Change Sysback Tape Defaults
Change Sysback CD/DVD Boot Defaults          Set Network
Install Defaults
```

Change Sysback Tape Boot Defaults

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

	[Entry Fields]	
Perform no-prompt installation	yes	+
THE FOLLOWING ARE REQUIRED FOR NOPROMPT INSTALL		
Console Device Name	[/dev/lft]	+
Console Terminal Type (if ascii)	[]	+
Non-rootvg Volume Group Option	Restore all VGs	+
Restore Device (if different than boot device)	[]	+
Backup Sequence Number (if tape)	[2]	#
Remove Sysback from foreign client after install?	yes	+
Remove Network Config from foreign client?	yes	+
Install Additional Device Driver Support?	None	+
Software Install Device	[]	+
Debug Logging?	yes	+
THE FOLLOWING WILL OVERRIDE INSTALL FILES ON THE BACKUP MEDIA:		
Post-Install Script	[]	
LVM Information File	[]	

F1=Help

F2=Refresh

F3=Cancel

F4=List

F5=Reset

F6=Command

F7=Edit

F8=Image

F9=Shell

F10=Exit

Enter=Do

Figure 16-4. The Change SysBack Tape Boot Defaults Menu

The fields have the following definitions:

Perform No-Prompt Installation?

Perform No-Prompt Installation specifies the client to be installed will be prompted. If this field is set to no, the installation menus will appear after a network boot. Otherwise, the install will take place after the network boot without prompting the user if all the required information has been provided. The default is no.

Console Device Name

To prevent the prompt shown prior to the installation menus that determines which console to be used for the installation, you must enter the name of the console device here. This may be either an LFT (graphical display) or TTY (ascii display) device. Examples are /dev/lft0 or /dev/tty0. If an LFT device exists on the client, it may also be selected by typing /dev/console. The default is none/blank.

Note: You must select the display, even for a promptless install. You will then be able to receive any error or warning messages and allow for prompts if the default information provided is insufficient to complete the install.

Console Terminal Type (if ascii)

If the console device is an ascii terminal, or tty device, you must select a specific terminal type. This ensures that installation menus, if required, are displayed with the correct terminal emulation. You may enter the device type or press F4 to display a list of all terminal types defined on the server and select from the list. Examples of common terminal types are "ibm3151", "vti925", and "vt100." The default is none/blank.

Non-rootvg Volume Group Option

The default is set at Restore Rootvg Only. The following is a description of each option.

Restore Rootvg Only

Only the rootvg volume group will be created and restored from the media, even if there are other volume groups defined in the backup. At the end of the install only the rootvg will be defined.

Restore All VGs

All volume groups that are included on the backup media will be created and restored. Volume groups that were defined on the original system but whose data was not included in the backup will be created but no data will be restored.

Import Non-Rootvgs

The rootvg volume group will be created and restored. All other volume groups will be imported from disks on the client. This option assumes that non-rootvg volume groups already exist on the client. You typically use this option when restoring the rootvg volume group after a system failure and no other volume groups have been affected.

Restore Device or File

The options which appear are those made available using **Add or Change Client Host Access to this Server** under the Remote Services menu. You must select an option from this list to prevent being prompted for an install device or file during the installation process. The default is none/blank. For more information on defining these resource, see Chapter 8, "Remote Services", on page 8-1.

Backup Sequence Number (if tape)

If the client is to be installed from tape, and the System Backup to be installed is not the first System Backup on the tape, enter the Backup Sequence Number. This number must be between 1 and the total number of System Backups on the tape media. The default is none/blank.

Remove Sysback from Foreign Client After Install

This yes or no field indicates whether to remove the SysBack program from the system after an installation. This is useful when the user has not purchased a license for the client that will be installed. The default is no.

Remove Network Config from Foreign Client

This yes or no field indicates whether to remove network specific information required to configure the host to the network. This option is useful when the machine installed was cloned from a backup image of a machine that is still present on the network. The default is no.

Install Additional Device Driver Support?

This option tells SysBack how much to install of what is contained in the media in the location specified by the **Software Install Device** option. The two options are:

Minimum

Selecting this option will install only those device support filesets identified by AIX when the system was booted. This information is obtained from the file `/tmp/devices.pkgs` which

is created by AIX when the system was booted. This file is not always 100% accurate regarding what device support is needed as some devices return invalid installp package names rather than individual filesets. In most cases, however, this is a reliable alternative to pre-installing all device support filesets on to a system prior to creating the backup image.

- All** Selecting this option tells SysBack to perform an install command against every item contained on the media in the specified location. This may include device support filesets or any other software that is located on the media.

Software Install Device

This option lets you specify a CDROM device name, a tape device name, or a NIM **LPPSOURCE** directory name. The NIM **LPPSOURCE** directory name provides additional device support to install during installation. This device support, if available in the specified location, will be installed in circumstances where the needed device support for this machine is contained in the boot image, not the backup image to be installed.

If this is a NIM Resource Network Boot, SysBack will automatically pull device support from the NIM **LPPSOURCE** specified when the Network Boot client was added regardless of whether this option is edited. For more information on configuring a NIM Resource Network Boot, see Chapter 13, “Network Boot/Installation Configuration”, on page 13-1.

Debug Logging

This yes or no field indicates whether to turn on debug logging operations for troubleshooting network boot and installation problems. The default is no.

Post-Install Script

Enter a filename to include a post installation script on the customized installation diskette. If it exists, this file will be executed at the end of the installation process before the system reboots. This can be used, for instance, to execute the sample script `/usr/lpp/sysback/scripts/install.post_rmnet` that removes the network configuration from the restored system data to prevent any prompts at the end of the SysBack installation process.

LVM Information File

Enter a filename to include an LVM information file on the customized installation diskette. Doing so replaces the LVM information contained on the backup and is typically used to apply many changes to the LVM information without requiring the user to do so using the installation menus. For more information about how to create a customized LVM information file, please refer to “Creating or Editing an LVM Information File” on page 16-18.

Changing SysBack CD/DVD Boot Defaults

Use the **Change SysBack CD/DVD Boot Defaults** menu to set boot defaults for CD or DVD media. Setting these defaults will let you minimize, possibly eliminate, user prompting during a CD/DVD boot or installation process. These defaults are stored in a file on the system. Therefore, you must set these options before the backup is executed, or boot only CD/DVD created, in order to ensure that this file

is included in the boot image. It is the file that is used during the boot and installation process that processes these specifications.

This is similar to the **Set Network Install Client Defaults** menu for network boot or installation processes.

To set the CD/DVD Boot Defaults:

Note: You may also access this same menu by using the following SMIT paths:

```

smitty sysback          Sysback Program Defaults
Change Sysback Program Defaults      Change Sysback Tape
Defaults                          Change Sysback CD/DVD Boot Defaults
                                Set Network Install Defaults

```

1. From the Utilities menu, select **Change SysBack CD/DVD Boot Defaults**.

Note: From a command line, type `smit sb_cfginstcd`.

2. The following screen is displayed:

Change Sysback CD/DVD Boot Defaults

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

	[Entry Fields]	
Perform no-prompt installation	yes	+
THE FOLLOWING ARE REQUIRED FOR NOPROMPT INSTALL		
Console Device Name	[/dev/lft]	+
Console Terminal Type (if ascii)	[]	+
Non-rootvg Volume Group Option	Restore all VGs	+
Restore Device (if different than boot device)	[]	+
Backup Sequence Number (if tape)	[2]	#
Remove Sysback from foreign client after install?	yes	+
Remove Network Config from foreign client?	yes	+
Install Additional Device Driver Support?	None	+
Software Install Device	[]	+
Debug Logging?	yes	+
THE FOLLOWING WILL OVERRIDE INSTALL FILES ON THE BACKUP MEDIA:		
Post-Install Script	[]	
LVM Information File	[]	

F1=Help
F5=Reset
F9=Shell

F2=Refresh
F6=Command
F10=Exit

F3=Cancel
F7=Edit
Enter=Do

F4=List
F8=Image

Figure 16-5. The Change SysBack CD/DVD Boot Defaults Menu

The fields have the following definitions:

Perform No-Prompt Installation?

Perform No-Prompt Installation specifies the client to be installed will be prompted. If this field is set to no, the installation menus will appear after a network boot. Otherwise, the install will take place after the network boot without prompting the user if all the required information has been provided. The default is no.

Console Device Name

To prevent the prompt shown prior to the installation menus that determines which console to be used for the installation, you must enter the name of the console device here. This may be either an LFT (graphical display) or TTY (ascii display) device. Examples are /dev/lft0 or /dev/tty0. If an LFT device exists on the client, it may also be selected by typing /dev/console. The default is none/blank.

Note: You must select the display, even for a promptless install. You will then be able to receive any error or warning messages and allow for prompts if the default information provided is insufficient to complete the install.

Console Terminal Type (if ascii)

If the console device is an ascii terminal, or tty device, you must select a specific terminal type. This ensures that installation menus, if required, are displayed with the correct terminal emulation. You may enter the device type or press F4 to display a list of all terminal types defined on the server and select from the list. Examples of common terminal types are "ibm3151", "vti925", and "vt100." The default is none/blank.

Non-rootvg Volume Group Option

The default is set at Restore Rootvg Only. The following is a description of each option.

Restore Rootvg Only

Only the rootvg volume group will be created and restored from the media, even if there are other volume groups defined in the backup. At the end of the install only the rootvg will be defined.

Restore All VGs

All volume groups that are included on the backup media will be created and restored. Volume groups that were defined on the original system but whose data was not included in the backup will be created but no data will be restored.

Import Non-Rootvgs

The rootvg volume group will be created and restored. All other volume groups will be imported from disks on the client. This option assumes that non-rootvg volume groups already exist on the client. You typically use this option when restoring the rootvg volume group after a system failure and no other volume groups have been affected.

Restore Device or File

The options which appear are those made available using **Add or Change Client Host Access to this Server** under the Remote Services menu. You must select an option from this list to prevent being prompted for an install device or file during the installation process. The default is none/blank. For more information on defining these resource, see Chapter 8, "Remote Services", on page 8-1.

Backup Sequence Number (if tape)

If the client is to be installed from tape, and the System Backup to be installed is not the first System Backup on the tape, enter the Backup

Sequence Number. This number must be between 1 and the total number of System Backups on the tape media. The default is none/blank.

Remove Sysback from Foreign Client After Install

This yes or no field indicates whether to remove the SysBack program from the system after an installation. This is useful when the user has not purchased a license for the client that will be installed. The default is no.

Remove Network Config from Foreign Client

This yes or no field indicates whether to remove network specific information required to configure the host to the network. This option is useful when the machine installed was cloned from a backup image of a machine that is still present on the network. The default is no.

Install Additional Device Driver Support?

This option tells SysBack how much to install of what is contained in the media in the location specified by the **Software Install Device** option. The two options are:

Minimum

Selecting this option will install only those device support filesets identified by AIX when the system was booted. This information is obtained from the file `/tmp/devices.pkgs` which is created by AIX when the system was booted. This file is not always 100% accurate regarding what device support is needed as some devices return invalid installp package names rather than individual filesets. In most cases, however, this is a reliable alternative to pre-installing all device support filesets on to a system prior to creating the backup image.

All Selecting this option tells SysBack to perform an install command against every item contained on the media in the specified location. This may include device support filesets or any other software that is located on the media.

Software Install Device

This option lets you specify a CDROM device name, a tape device name, or a NIM **LPPSOURCE** directory name. The NIM **LPPSOURCE** directory name provides additional device support to install during installation. This device support, if available in the specified location, will be installed in circumstances where the needed device support for this machine is contained in the boot image, not the backup image to be installed.

If this is a NIM Resource Network Boot, SysBack will automatically pull device support from the NIM **LPPSOURCE** specified when the Network Boot client was added regardless of whether this option is edited. For more information on configuring a NIM Resource Network Boot, see Chapter 13, “Network Boot/Installation Configuration”, on page 13-1.

Debug Logging

This yes or no field indicates whether to turn on debug logging operations for troubleshooting network boot and installation problems. The default is no.

Post-Install Script

Enter a filename to include a post installation script on the customized

installation diskette. If it exists, this file will be executed at the end of the installation process before the system reboots. This can be used, for instance, to execute the sample script `/usr/lpp/sysback/scripts/install.post_rmnet` that removes the network configuration from the restored system data to prevent any prompts at the end of the SysBack installation process.

LVM Information File

Enter a filename to include an LVM information file on the customized installation diskette. Doing so replaces the LVM information contained on the backup and is typically used to apply many changes to the LVM information without requiring the user to do so using the installation menus. For more information about how to create a customized LVM information file, please refer to “Creating or Editing an LVM Information File” on page 16-18.

Changing the Read Permission on a Disk Image File

When you back up to a disk image file, you can set the read permission of the file to allow only the original host and/or original user to read from the file. You might need to change this permission at a later time if, for instance, you need to use an image file with “original host only” permission as a network installation image for other systems.

Using the **Change Read Permission on a Disk Image File** option, you can change the owner of the file (host and/or user), the backup description, if any, or the host or user read permission.

Only the following users have permission to change the read permission of a disk image file:

- Root user on the system where the file physically resides
- Root user on the system from which the file originated
- User on the system who originally wrote the file

To change the permissions of an existing disk image file:

1. From the Utilities menu, select **Change Read Permission on a Disk Image File**.
2. Select the disk image file you want to change from the list displayed. This list displays all the files in the backup or installation image directories assigned to the current user.

Root users can change files that are not on this list. To do this, select any file from this list and change it on the **Change Read Permission on a Disk Image File** screen that follows.

3. The following screen is displayed:

Change Read Permission on a Disk Image File

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

	[Entry Fields]
Hostname (where file resides)	hambone.austin.ibm.com
* File Name	[/sysback.images/fatrat> +/
Hostname (owner of file)	[fatrat]
User name (owner of file)	[root]
Host read permission	all hosts +
User read permission	all users +
User description	[]

F1=Help

F2=Refresh

F3=Cancel

F4=List

F5=Reset

F6=Command

F7=Edit

F8=Image

F9=Shell

F10=Exit

Enter=Do

Figure 16-6. The Change Read Permission on a Disk Image File Menu

The fields have the following meanings:

Hostname (where file resides)

The name of the host where the file resides, if a remote file was selected on the prior selection screen. You cannot change this field on this screen.

File name

The name of the file selected on the prior screen. You cannot change this field on this screen.

Hostname (owner of file)

Default=(current owner). The hostname.

Note that, if the **Host read permission** field is set to “this host only”, changing the owner of the file to a new host prevents the original host from accessing the file. The root user on the server in which the file physically resides can always access the file.

User name (owner of file)

Default=(current owner). The user name.

Note that, if the **User read permission** field is set to “this user only”, changing the owner of the file to a new user will prevent the original user from accessing the file. The root user on the host that owns the file, or the root user on the server in which the file physically resides will always be able to access the file.

Host read permission

Default=(current host read permission). Press Tab to change the field from its current value to a new value. The possible values are:

this host only The file can be read only by the host that owns the file. Either the root user on that host or the user who owns the file, if different, can read it. The root user on the server where the file physically resides can also access the file.

all hosts The file can be read by any host on the network. You can still limit access permission by the user name.

User read permission

Default=(current user read permission). Press Tab to change the field from its current value to a new value. The possible values are:

this user only The file can only be read by the user who owns the file. The root user on the host that owns the file, or root on the server on which the file physically resides, can also access the file. Limit read permission of the file to only the host that owns the file. If not, the file can be read by this user from any host on the network.

all users The file can be read by any user. The access permission can be limited to the host that owns the file. If not, any user on the network can read the file.

User description

Default=(current user description, if any). The backup description specified by the user when the backup was created. This description, up to 60 characters, can be changed by entering the new description in this field. Do not include single (') or double (") quotes in this field.

4. Press Enter to change the file or press F3 key at any time to exit without saving any changes.

Creating or Editing an LVM Information File

An *LVM information file* is created by the **mkvginfo** command as part of all SysBack backups that contain LVM (logical volume manager) information. This file is then used either when reinstalling the system from a backup or recreating volume groups, logical volumes, or filesystems from a backup.

You might want to create your own LVM information file and tailor it to your needs. This customized LVM information file can then be placed on the backup by using the **-g** flag to either the **sysback**, **mkvgback**, **mkjfsback** or **mklvback** commands. The customized LVM information file can also be written to a diskette and used to replace the information on an existing system backup during a system installation. Refer to “Creating a Custom Installation Diskette” on page 16-19 in this chapter for additional details.

To edit an existing LVM information file or create a new LVM information file from the information on the current system and edit the new file:

1. From the Utilities menu, select **Create or Edit an LVM Information File**.
2. Enter the name of an existing file or the name of a new file to create.
3. Select the type of backup for the new file. Choose from the following types:

S	System Backup
P	Power System Backup
V	Volume Group Backup
L	Logical Volume or Filesystem Backup

Select the type of file to create based on the backup the file will be used with. If you select a type that does not match the actual backup media, errors can prevent the backup media from being restored properly.

4. If you are creating a new file and you specified the system, power, or volume group backup type, select the volume group whose data is on the backup. To select a single volume, highlight the volume group and press Enter. To select multiple volume groups, highlight each volume group and press F7. When you have selected all entries, press Enter to continue.

It is important to indicate in this field which volume groups are actually included on the backup. Not doing so prevents the volume group data from being restored during a system installation. Regardless of which volume groups are included in the backup data, any volume group can be recreated from this backup, either during the system installation process or when recreating volume groups on an active system.

The LVM file is created or checked for consistency with the system configuration, and then a screen similar to the following is displayed:

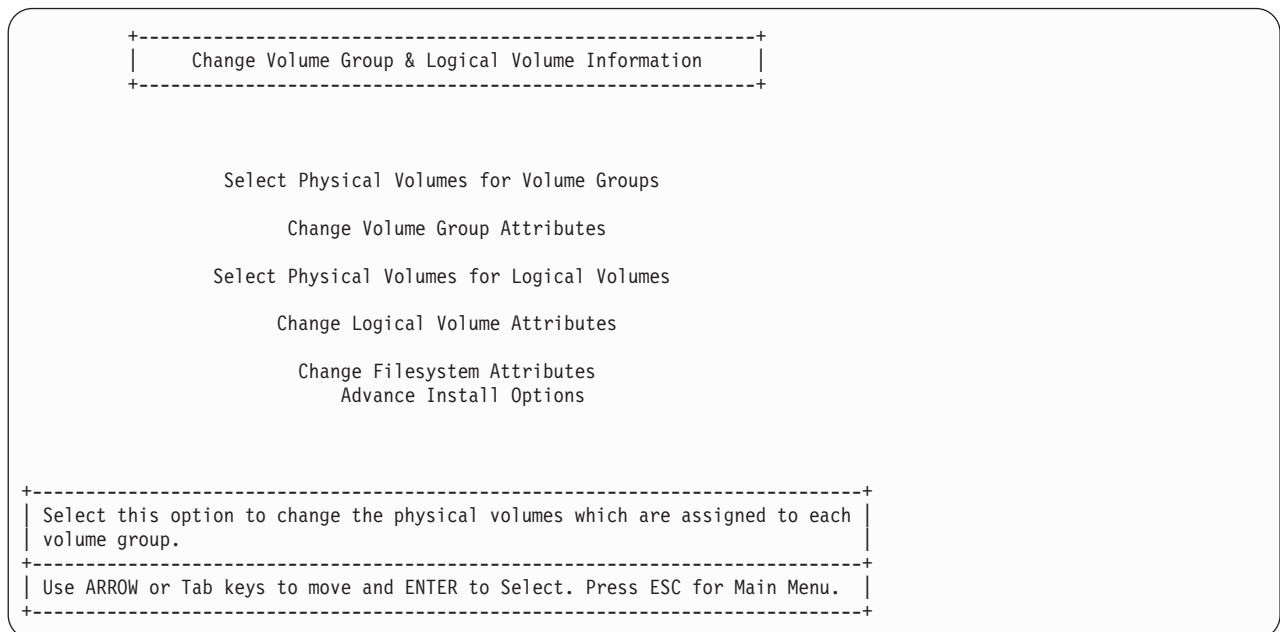


Figure 16-7. The Change Volume Group & Logical Volume Information Menu

The options for volume groups are not displayed when you select to create or edit a file for a logical volume or filesystem backup. Also, if this is a power backup, the option for changing filesystem information does not appear. These menus provide options for changing virtually all attributes for volume groups, logical volumes, and filesystems. This process is identical to that for reinstalling a system from a system backup. Therefore, in both cases, the detailed steps for changing this information is provided in Chapter 11, “Changing the Volume Group, Logical Volume and Filesystem Attributes”, on page 11-1.

Creating a Custom Installation Diskette

You can customize the system installation process by using a customized installation diskette.

To create a customized installation diskette:

1. From the Utilities menu, select **Create a Custom Installation Diskette**.

Note: From the command line, type `smit sb_mkinstdskt`.

2. The following screen is displayed:

Create Custom Installation Diskette

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

	[Entry Fields]	
Output device name	[/dev/fd0]	+/ +
Format diskettes before copying?	no	+
Filename of LVM Information File	<input type="text"/>	+
Filename of Pre-Installation Script	<input type="text"/>	+
Filename of Post-rootvg Install Script	<input type="text"/>	+
Filename of Post-Installation Script	<input type="text"/>	+

F1=Help
F5=Reset
F9=Shell

F2=Refresh
F6=Command
F10=Exit

F3=Cancel
F7=Edit
Enter=Do

F4=List
F8=Image

Figure 16-8. The Create Custom Installation Diskette Menu

The fields have the following meanings:

Output device name

Default=diskette device (/dev/fd0). A diskette drive name. If there is more than one diskette drive on your system, press F4 to display the available diskette drives and select a drive from the list.

Format diskette before copying?

Default=no. If the diskette in the drive has not been formatted, press Tab to change this to "yes."

Filename of LVM Information File

Enter a filename to include an LVM information file on the customized installation diskette. Doing so replaces the LVM information contained on the backup and is typically used to apply many changes to the LVM information without requiring the user to do so using the installation menus.

Filename of Pre-installation script

Enter a filename to include a pre-installation script on the customized installation diskette. If it exists, this file is executed prior to the installation menus appearing on the screen. This might be used, for instance, to restore other information from the diskette or to perform some special system configuration not ordinarily performed by the installation process.

Filename of Post-rootvg installation script

Enter a filename to include a post-rootvg installation script on the customized installation diskette. If it exists, this file is executed after the files for the rootvg volume group are restored.

This is commonly used to execute the sample script
/usr/lpp/sysback/scripts/install.postroot_hwmigrate, provided with

SysBack, that performs an automatic installation of device code from CD-ROM not already included in the system restored from the backup media.

Filename of Post installation script

Enter a filename to include a post installation script on the customized installation diskette. If it exists, this file will be executed at the end of the installation process before the system reboots. This can be used, for instance, to execute the sample script `/usr/lpp/sysback/scripts/install.post_rmnet` that removes the network configuration from the restored system data to prevent any prompts at the end of the SysBack installation process.

You can find more information on the sample installation scripts provided with SysBack in Appendix D, “Creating Scripts for Customizing the System Backup and Install Process”, on page D-1.

After this diskette has been created, insert the diskette during the system boot process. It is read automatically, and any of the above information files provided are used during the installation process, overriding the same information on the backup media if it exists.

Changing SysBack Program Defaults

Use the **Change SysBack Program Defaults** option to tailor the behavior of certain functions of SysBack. These include the underlying format of the backups, how read errors are handled when reading backup media, and attributes used to tune network performance. This section describes the various parameters that can be changed and the reasons you might choose to do so.

Normally, you do not need to change the default behavior of SysBack. These parameters should not be changed except by experienced users who understand the reasons for doing so, as described below.

To access the menus to change the SysBack program defaults, select **Change SysBack Program Defaults** on the Utilities menu. You can also access these menus by typing `smit sb_chgsettings` at a command line.

The following screen is displayed. The values shown are the system defaults. If you changed the attributes previously, those values are displayed.

Note: You may also access this same menu by using the following SMIT paths:

```
smitty sysback          Sysback Program Defaults
Change Sysback Program Defaults          Change Sysback Tape
Defaults                          Change Sysback CD/DVD Boot Defaults
                                Set Network Install Defaults
```

Change Sysback Program Defaults

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

[MORE...4]

Filesystem Data Backup Command

[Entry Fields]

Backup/Restore

+

END OF TAPE (EOT) PROCESSING

Program For EOT on Write Operations.

Program For EOT on Read Operations.

Email Address For EOT on Write Operations.

Email Address For EOT on Read Operations.

ERROR HANDLING SETTINGS

Number of data read errors before read failure

Number of data sync errors before read failure

Maximum number of retries on read errors

Pad missing data with NULLS after sync error?

[50]

[50]

[2000]

yes

#

#

#

+

SYSBACK NETWORK SETTINGS

Data Buffer size

TCP Send Buffer size (in bytes)

TCP Receive Buffer size (in bytes)

Force TCP to always send data immediately?

no

#

#

#

+

[BOTTOM]

F1=Help

F2=Refresh

F3=Cancel

F4=List

F5=Reset

F6=Command

F7=Edit

F8=Image

F9=Shell

F10=Exit

Enter=Do

Figure 16-9. The Change SysBack Program Defaults Menu

The following sections describe the options available from the Change SysBack Program Defaults menu.

Backup Format Settings

This section contains options for changing the format of the backup itself. The default format is “Backup/Restore”, or the AIX **backup** and **restore** command format.

Although SysBack creates a data format to store information about the backup contents and system information and to enable multi-copy and striped backups, the underlying command used to read and write files within the filesystems is the AIX **backup** command.

SysBack now enables the user to use either the AIX **backup** command or the AIX **tar** command for backing up and restoring filesystem data. When any SysBack backup is restored, SysBack automatically detects the backup type and uses the appropriate corresponding restore command to restore the data.

Note: The **backup** command is the default and should not be changed unless another command provides function that the backup command does not.

To change the filesystem backup command, press Tab to scroll through the options. You can also press F4 to display a list of the values. The default is “backup/restore.”

The **backup** command is used because of its flexibility over other commands and because it backs up data regarding files such as the *access control list* (ACL) and the *trusted computing base* (TCB).

The **backup** command, however, has changed over time in how it backs up and restores “sparse” files. A *sparse file* is a file in which blocks of data have been written non-sequentially, leaving unallocated blocks in the middle of a file. Previous levels of the backup command did not preserve this sparseness, and a sparse file, when restored, expands to include all blocks in the middle of the file, often causing a filesystem to inadvertently run out of space. The **backup** command was later changed to preserve this sparseness, but this is often a problem for customers experiencing the opposite affect.

If a file is created and all blocks are allocated by writing nulls, or “0s,” throughout the file, these blocks of data are not preserved during a restore, because the goal is to preserve sparseness. Because of this, a large file might be restored to a very small size.

SysBack enables you to select the command you want to use to perform backups. This can be either the AIX **backup** and **restore** commands (which preserve sparseness) or the **tar** command (which does not).

End of Tape (EOT) Processing Options

This feature will allow you to specify a network e-mail address, or program to execute, when the end of volume is reached during backup and restore operations.

For multi-volume backups, each time the end of tape is reached the configured option will be executed. If you configure this option and have an autoloading device that automatically loads the next tape for you, these actions will still be executed even if no action is required. An example might be in an environment where you would like an e-mail sent at each tape change, even though the library is changing tape for you in order to have an easy reference indicating the number of volumes in any given backup.

This function is particularly useful in environments that have robotic libraries that require special commands or software to mount and dismount tape volumes. Since SysBack does not interact or control the medium changer in a library, this allows you to create a script that will issue the commands for SysBack for each tape change during a backup or restore.

There are 4 options that can be set to affect the end of tape processing. These are configured on the SysBack server where the tape library is physically attached.

Program For EOT on Write Operations.

Specify an e-mail address to send the message to when end of tape has been reached (triggered by the sbwrite command). This option only affects backup operations.

Program For EOT on Read Operations.

Specify an e-mail address to send the message to when end of tape has been reached (triggered by the sbread and sbfwd commands). This option only affects restore, list, and verify operations. The e-mail title will be like this:

SysBack Tape Change on host "sysback1" for Tape Drive /dev/rmt0 Tape 2

The body would contain this information:

```
HOST sysback1
TAPE_DRIVE /dev/rmt0
TAPE 2
```

Both of these options assume that your e-mail address is valid and that your system is configured such that the e-mail can be sent. SysBack is sending the e-mail via the AIX mail command. It is the customer's responsibility to properly configure their mail options. This might be useful when you would like and e-mail sent to a particular Computer Operator each time a tape needs to be changed, or simply for record keeping purposes.

Email Address For EOT on Write Operations.

Specify this option to force SysBack to execute the specified script/program when the end of tape is reached (triggered by the sbwrite and sbfwd commands). You must specify the fully qualified path to the script/program and it must be present on the same physical machine as where the tape drive / library is located. This option only applies to backup operations.

Email Address For EOT on Read Operations.

Specify this option to force SysBack to execute the specified script/program when the end of tape is reached (triggered by the sbread command). You must specify the fully qualified path to the script / program and assumes that it is present on the same physical machine as where the tape drive or library is located. This option only applies to restore operations.

Both of these options would be used in a situation whereby you did not have an autoloading library, but instead a robotic library that requires special commands to move the robot arm for picking up and moving tapes. You could write your own script or program to manipulate the tapes when the end of volume is reached. Three command line arguments will be passed to your program. You may take advantage of them if you choose. They are:

-
- \$1** This argument represents the device that requires the tape change. The value will be in the form of /dev/rmt0.
-
- \$2** This argument represents the hostname of the client whose data is being backed up. It should be in the form of what is returned by running the "hostname" command on that client
-
- \$3** This argument represents the value of the next tape to load. For example, at the end of tape 1, this value would be "2" since the 2nd volume that should loaded.

As an example configuration, let's assume that when the backup's "sbwrite" command hits the end of tape of tape 1, and needs to span to tape 2, (assuming that this is only a 2 tape backup), you would specify the program name in SMIT like so:

```
PROGRAM_WRITE  change_tape
```

Therefore, when the end of the first tape was reached on host sysback1, SysBack would execute this command:

```
change_tape /dev/rmt0 sysback1 2
```

Where change_tape might be a shell script like this:

Note: The `tapeutil` command is a sample program that come with the IBM **Atape.driver** file set. This is the device driver that controls IBM Magstar[®] tape devices. This is not a SysBack command.

```
#!/bin/ksh
DEVICE=$1
HOST=$2
TAPE=$3
case $TAPE in
2) tapeutil -f /dev/smc0 move 23 10
   tapeutil -f /dev/smc0 move 11 23
;;
3) tapeutil -f /dev/smc0 move 23 11
   tapeutil -f /dev/smc0 move 12 23
;;
4) tapeutil -f /dev/smc0 move 23 12
   tapeutil -f /dev/smc0 move 13 23
;;
5) tapeutil -f /dev/smc0 move 23 13
   tapeutil -f /dev/smc0 move 14 23
;;
esac
```

When performing remote backups, the user who will be running your program or script is the `sbnet` user. You will need to accommodate this accordingly if there are commands in your program or script that require root user authority. Also, the read and execute permissions on your program or script must be set to allow the `sbnet` user to run it.

Error Handling Settings

This section provides options for controlling the way read errors are handled when reading from SysBack backup media. Although SysBack itself provides a reliable backup, the media on which the backup is placed can sometimes become corrupt.

The fields have the following meanings:

Number of data read errors before read failure

Default=50. When SysBack encounters a read error from the media device driver, by default, it attempts to read up to the number of times specified in the **Maximum number of retries on read errors** field. If SysBack is unable to read the data, a read error is produced, and SysBack either skips the missing data entirely or pads the missing data with NULL bytes, as defined by the **Pad missing data with NULLs after sync errors** field.

This option enables you to specify the maximum number of read errors that are produced before the backup fails. Specify any number up to 32768 in this field or use a zero (0) to indicate that the reading fails after the first read error.

Number of data sync errors before read failure

Default=50. The backup is read for each buffer, defined by the buffer size of the backup. At the beginning of each buffer is a special key that ensures that the data is being read at the correct point. A “data sync” error occurs when the key is not encountered or the key has an incorrect sequence number.

When a sync error occurs, SysBack either skips the missing data altogether or pad the missing data with NULL bytes, as defined by the **Pad missing data with NULLs after sync errors** field.

This field determines the maximum number of sync errors that can occur before the reading fails. The value of this field can be any number up to 32768. Using a value of zero (0) indicates that the reading should abort after the first sync error.

Maximum number of retries on read errors

Default=2000. When a read error occurs, by default SysBack attempts to reread the same buffer of data up to the number of times specified by this field. The reading fails when a read error occurs and has been retried the number of times indicated. You can enter a number up to 32768. An entry of zero (0) indicates that no retries should be attempted.

Note: Most tape devices, including 8MM tape drives, return an error very quickly when a read error occurs and allows retries to be attempted from the same data location. Others, such as DDS 4MM tape drives, take up to 2 minutes to return from a read error. These tape devices also do not allow read retries, but still take two minutes to return from an attempt. Therefore, for these, and similar devices, set this value to zero (0), because retries are not supported and any attempts appear to pause the reading indefinitely.

Pad missing data with NULLs after sync errors?

Default=yes. When a data sync error occurs, assuming the reading is set up to continue, the missing data is padded with NULL bytes by default. This is to ensure that, although the data has been altered, it remains in the correct alignment.

Note: It is very important for the data to remain in the correct alignment when restoring raw logical volume backups. If you do not pad sync errors with NULL bytes, all of the data following the error is restored to a different location than expected. Volume group, filesystem, and file/directory backups use an underlying restore command that is capable of resynchronizing when there is missing data in the data stream. Therefore, the value of this field is less relevant when restoring from these backup types. However, the restore command sometimes fails when it encounters a large stream of NULL bytes. In this case, change this value to "no."

SysBack Network Settings

By tuning certain network parameters, you can increase the performance of SysBack backups and restores. You can set certain values that affect network performance during SysBack backups and restores without affecting network performance of other processes using the same network.

Note: Do not change the network settings using this option unless you are familiar with network tuning. Also, you must apply the same settings to both the SysBack server and client hosts.

In most situations, the default settings are adequate. The settings appropriate for achieving the greatest performance on different systems and networks vary widely, so no specific guidance can be given here. Refer to Appendix E, "Device/System-Specific Information", on page E-1 for any specific recommendations.

The following fields are displayed in the SysBack Network Settings section:

Data buffer size

Default=32768 (32 Kbytes). The size of the buffer of data that is written to the network socket in a single write operation.

TCP Send Buffer size (in bytes)

Default=16384 (16 Kbytes). The TCP “send buffer” size, equivalent to the *tcp_sendspace* parameter of the AIX “**no**” command. If the send buffer size is greater than 64 Kbytes, the RFC1323 TCP parameter, which is equivalent to the *rfc1323* parameter of the AIX “**no**” command, is enabled automatically.

TCP Receive Buffer size (in bytes)

Default=16384 (16 Kbytes). The TCP “receive buffer” size, equivalent to the *tcp_recvspace* parameter of the AIX “**no**” command. If the receive buffer size is greater than 64 Kbytes, the RFC1323 TCP parameter, which is equivalent to the *rfc1323* parameter of the AIX “**no**” command, is enabled automatically.

Force TCP to always send data immediately?

Select “yes” by pressing Tab if you want to send TCP packets immediately. Otherwise, a value of “no” indicates that small amount of data should be collected into single packets before being sent.

When all entries are completed, press Enter to apply the changes.

Note: The changes take affect only during SysBack backups, verifies, and restores, and have no affect on other system network operations. The changes applied here do not apply to a SysBack system installation; it is not possible to query the values set during the installation process.

Logging

This menu provides options for manipulating the SysBack Activity Log. For more information related to this topic, please refer to Chapter 19, “Activity Logging”, on page 19-1.

Chapter 17. Copying Backups to a New Media Type

You can transfer a backup that exists in one media source to another. For example, if you normally perform up your SysBack System Installation Image backups to files on disk, but later need to make a bootable backup tape out of them, you would use the **Device to Device Copy** menus. There are three different menu options:

- Copy Backup Disk Image or CD/DVD to Tape
- Copy Backup Tape to Backup Disk Image
- Copy Backup Tape to Backup Tape

These three options provide the ability to:

- Copy backups from files on disk to tape
- Copy backups from CD / DVD to tape
- Copy backups from tape to files on disk
- Copy backups from tape to tape
- Copy backups from tape to disk, and then burn them back to CD or DVD

Note: These utilities do not support backups stored in a TSM server, or using a TSM server as the output device.

To access the **Device to Device Copy** menus:

1. At a command line, type smitty sysback.
2. Select **Device to Device Copy** which will display the following screen:

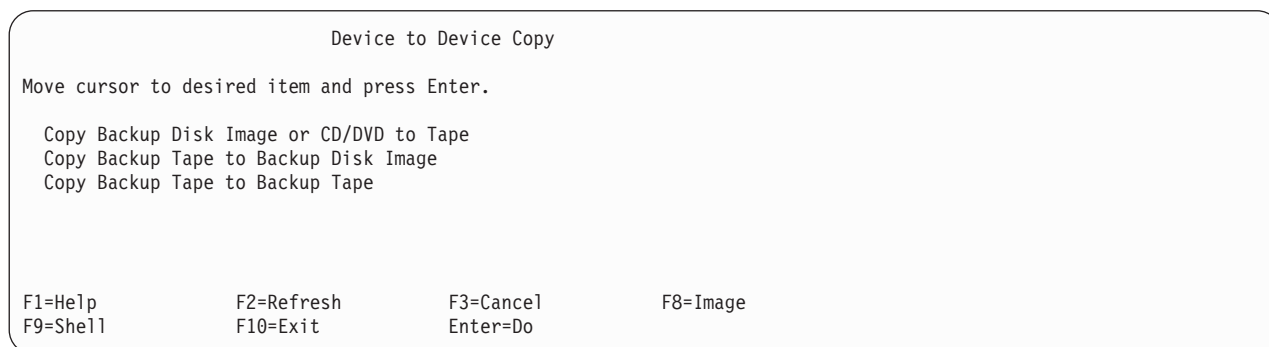


Figure 17-1. The Device to Device Copy Menu

Copy Backup from Disk Image or CD/DVD to Tape

If you select the **Copy Backup from Disk Image or CD/DVD to Tape** menu:

Note: These utilities do not support backups stored in a TSM server, or using a TSM server as the output device.

1. Select the Full System Disk Image Backup file or CD / DVD device where the backup is stored.
2. Select tape drive or virtual device to use as the output device.

You will be presented with the following menu:

Copy Backup Disk Image or CD/DVD to Tape

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

[TOP]	<div style="text-align: right; margin-bottom: 10px;">[Entry Fields]</div> <div> <div>INPUT DEVICE OPTIONS:</div> <div>Input Device or file name /dev/cd0</div> </div>
	<div> <div>OUTPUT DEVICE OPTIONS:</div> <div>Output hostname of server</div> <div>Output Device or Directory /dev/rmt0</div> <div>Output device buffer size (in Kbytes) [64] #</div> <div>Compress data before writing to output media? no +</div> <div>Report output type progress indicator +</div> <div>Use Existing Bootimage? no +</div> <div>Platform/kernel type for tape boot image [rspc/MP] +</div> <div>Network install support to include [] +</div> <div>Rewind tape before starting copy? yes +</div> <div>Forward to End of Tape before starting copy? no +</div> </div>
	<div>Device name for remote volume prompt []</div>
[BOTTOM]	

F1=Help	F2=Refresh	F3=Cancel	F4=List
Esc+5=Reset	F6=Command	F7=Edit	F8=Image
F9=Shell	F10=Exit	Enter=Do	

Figure 17-2. The Copy Backup Disk Image or CD/DVD to Tape Menu

The fields have the following meaning:

Input Device or file name

Specify the local directory path or device name where the backup file images exist. For example: /dev/cd1 or /backup_images/SB.hostname.date.TOC.

Output hostname of server

Specify the hostname of the system which contains the tape drive or virtual device specified by the **Output device or Directory** field.

Output device or directory

Specify the name of the tape drive or virtual device that will be the output of this operation. For example: /dev/rmt0.

Output device buffer size (in Kbytes)

Specify the buffer size to use when storing data to the output device. The default is 64k. The buffer size indicates the amount of data that is written to the output device in a single output operation. Using a buffer size that best optimizes a particular device can have significant performance advantages.

Note: The larger the buffer size, the more memory will be used by the system during the operation.

Compress data before writing to output media?

Specifying this option will cause the data to be compressed by this system prior to writing to the backup device. You should not compress data if the device you are writing to has built-in compression capability, unless you are writing the backup to a remote host and wish to send less data over the network.

Note: Compressing the backup using software and device compression may cause the data to actually grow in size, as well as, to corrupt it.

Report output type

Specify whether to display a progress indicator during the copy process or to display errors only.

Use Existing Boot image?

Specify whether to use the existing boot image on the tape such as when transferring this backup image to a SysBack "Boot Only" tape. This may only be used with Full System backups.

Note: This option should be set to "no" when you are also specifying **Forward to End of Tape before starting copy?** to "yes".

Platform/kernel type for tape boot image

Specify the kernel and platform type to use when creating the boot image. Valid kernel options are: **mp** for multiprocessor or **up** for uniprocessor. Valid platform options are: **rspc**, **rs6k**, or **chrp**. The option chosen should match the kernel and platform type of the system that will boot from this backup tape. The default is the kernel and platform type of the machine initiating this process.

Note: This may only be used with Full System backups.

Network install support to include

Specify the type of network adapter support that should be included in the boot image. This would be utilized in situations where you boot from this tape but may install from an image or tape located on a remote machine on the network. Valid options are: **ethernet**, **token-ring**, or **FDDI**.

Note: This may only be used with Full System backups.

Rewind tape before starting copy?

Specify whether to rewind the output device before starting the process. Use this option when you have manually positioned the tape at the end of a backup sequence, or when you want to overwrite any data already on the tape.

Forward to End of Tape before starting copy?

Specify whether to forward to the end of the last image on the output device before beginning this operation. This option would be used to stack multiple backups on to a single tape for example.

Device name for remote volume prompt

Specify this option when backing up to a remote or local server to indicate the name of a terminal device on which to display volume prompt messages for multi-volume operations.

3. Once you have entered your selections, press the Enter key to begin the process.

Copy Backup Tape to Backup Disk Image

If you select the **Copy Backup from Tape to Disk Backup** menu:

Note: These utilities do not support backups stored in a TSM server, or using a TSM server as the output device.

1. Select the tape or virtual device where the backup is stored.
2. Select directory to use as the output device.

You will be presented with the following menu:

Copy Backup Tape or Virtual Device to Backup Disk Image

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

[TOP]

INPUT DEVICE OPTIONS:

Input Device or file name

Backup Sequence Number

Rewind tape before starting copy?

[Entry Fields]

/dev/rmt0

[]

yes

OUTPUT DEVICE OPTIONS:

Output hostname of server

Output Device or Directory

Output device buffer size (in Kbytes)

Compress data before writing to output media?

Report output type

Backup file ID

Dynamically Created Backup file ID

Overwrite existing backup with same ID?

CD/DVD media Size

/usr/lpp/sysback/imag>

[64]

no

progress indicator

[03261329]

no

no

[]

Device name for remote volume prompt

[]

[BOTTOM]

F1=Help

F2=Refresh

F3=Cancel

F4=List

Esc+5=Reset

F6=Command

F7=Edit

F8=Image

F9=Shell

F10=Exit

Enter=Do

Figure 17-3. The Copy Backup Tape or Virtual Device to Backup Disk Image Menu

The fields have the following meaning:

Input device or file name

Specify the locally attached tape drive or virtual device name where the backup file images exist. For example: /dev/rmt0.

Backup Sequence Number

Specify the backup image to position to on the input device before beginning the process. For example, if you had 3 backups stacked on to the same tape, and you would like to copy backup 2 to the output device, specify "2" in this field.

Rewind tape before starting copy?

Specify whether to rewind the input device before starting the process.

Output hostname of server

Specify the hostname of the system which contains the tape drive or virtual device specified by the **Output device or Directory** field.

Output device or Directory

Specify the directory name that will be the output of this operation. For example: /backup_copies.

Output device buffer size (in Kbytes)

Specify the buffer size to use when storing data to the output device. The default is 64k. The buffer size indicates the amount of data that is written to the output device in a single output operation. Using a buffer size that best optimizes a particular device can have significant performance advantages.

Note: The larger the buffer size, the more memory will be used by the system during the operation.

Compress data before writing to output media?

Specifying this option will cause the data to be compressed by this system prior to writing to the backup device. You should not compress data if the device you are writing to has built-in compression capability, unless you are writing the backup to a remote host and wish to send less data over the network.

Note: Compressing the backup using software and device compression may cause the data to actually grow in size, as well as, to corrupt it.

Report output type

Specify whether to display a progress indicator during the copy process or to only display errors if encountered.

Backup file ID

A backup file ID is used to create a unique file name when writing a backup to a disk file. The default ID contains the current date and time. You may change this field to any value you desire to describe the backup. If you choose an ID already in use in the specified directory, you must also choose to "Overwrite existing backup with same ID" option or the backup transfer will fail.

Dynamically Create Backup file ID

This option may be used instead of combining the "Backup File ID" and "Overwrite existing backup with same ID?" options to generate a dynamically created backup file ID based on the date and time of the command's execution.

Overwrite existing backup with same ID?

If the specified "Backup file ID" is already used to name a backup in the specified directory, and you are not using the "Dynamically Create Backup file ID" option, you must use this flag to allow the prior backup to be overwritten. Otherwise, you must choose another unique ID or the backup transfer process will not continue.

CD/DVD media Size

Specifying a size value will format this backup image to file in such a manner as to burn it to CD or DVD at a later time. Specify the media size in MB. If the size of your media is double sided, only specify the size of one side of the media, not the total aggregate.

Device name for remote volume prompt

Specify this option when backing up to a remote or local server to indicate the name of a terminal device on which to display volume prompt messages for multi-volume operations.

3. Once you have entered your selections, press the Enter key to begin the process.

If you would like to copy a backup from tape to CD / DVD, simply complete this process first to transfer the backup to a disk image file. Then, you may use the SysBack Backup to CD / DVD feature to burn the existing backup image to disk. To learn more about the Backup to CD / DVD options and their meaning, please refer to Chapter 5, "Backups to CD or DVD", on page 5-1.

Copy Backup Tape to Backup Tape

If you select the **Copy Backup Tape to Backup Tape** menu:

Note: These utilities do not support backups stored in a TSM server, or using a TSM server as the output device.

1. Select the tape or virtual device where the backup is stored.
2. Select the tape or virtual device to use as the output device.

You will be presented with the following menu:

Copy Backup Tape to Backup Tape

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

[TOP]	[Entry Fields]
INPUT DEVICE OPTIONS:	
Input Device or file name	/dev/rmt0
Backup Sequence Number	[] #
Rewind tape before starting copy?	yes +
OUTPUT DEVICE OPTIONS:	
Output hostname of server	
Output Device or Directory	/dev/rmt1
Output device buffer size (in Kbytes)	[64] #
Compress data before writing to output media?	no +
Report output type	progress indicator +
Use Existing Bootimage?	no +
Platform/kernel type for tape boot image	[rspc/MP] +
Network install support to include	[] +
Rewind tape before starting copy?	yes +
Forward to End of Tape before starting copy?	no +
Device name for remote volume prompt	[]
[BOTTOM]	
F1=Help	F2=Refresh
Esc+5=Reset	F6=Command
F9=Shell	F10=Exit
F3=Cancel	F7=Edit
F4=List	F8=Image
Enter=Do	

Figure 17-4. The Copy Backup Tape to Backup Tape Menu

The fields have the following meanings:

Input Device or file name

Specify the locally attached tape or virtual device name where the backup file images exist. For example: /dev/rmt0.

Backup Sequence Number

Specify the backup image to position to on the input device before beginning the process. For example, if you had 3 backups stacked on to the same tape, and you would like to copy backup 2 to the output device, specify "2" in this field.

Rewind tape before starting copy?

Specify whether to rewind the input device before starting the process. Use this option when you have manually positioned the tape at the end of a backup sequence.

Output hostname of server

Specify the hostname of the system which contains the tape drive or virtual device specified by the **Output device or Directory** field.

Output Device or directory

Specify the name of the tape drive or virtual device that will be the output of this operation. For example: /dev/rmt0.

Output device buffer size (in Kbytes)

Specify the buffer size to use when storing data to the output device.

The default is 64k. The buffer size indicates the amount of data that is written to the output device in a single output operation. Using a buffer size that best optimizes a particular device can have significant performance advantages.

Note: The larger the buffer size, the more memory will be used by the system during the operation.

Compress data before writing to output media?

Specifying this option will cause the data to be compressed by this system prior to writing to the backup device. You should not compress data if the device you are writing to has built-in compression capability, unless you are writing the backup to a remote host and wish to send less data over the network.

Note: Compressing the backup using software and device compression may cause the data to actually grow in size, as well as, to corrupt it.

Report output type

Specify whether to display a progress indicator during the copy process or to only display errors if encountered.

Use existing Boot image?

Specify whether to use the existing boot image on the tape such as when transferring this backup image to a SysBack "Boot Only" tape. This may only be used with Full System backups.

Note: This option should be set to "no" when you are also specifying **Forward to End of Tape before starting copy?** to "yes".

Platform / kernel type for tape boot image

Specify the kernel and platform type to use when creating the boot image. Valid kernel options are: **mp** for multiprocessor or **up** for uniprocessor. Valid platform options are: **rspc**, **rs6k**, or **chrp**. The option chosen should match the kernel and platform type of the system that will boot from this backup tape. The default is the kernel and platform type of the machine initiating this process.

Note: This may only be used with Full System backups.

Network install support to include

Specify the type of network adapter support that should be included in the boot image. This would be utilized in situations where you boot from this tape but may install from an image or tape located on a remote machine on the network. Valid options are: **ethernet**, **token-ring**, or **FDDI**.

Note: This may only be used with Full System backups.

Rewind tape before starting copy?

Specify whether to rewind the output device before starting the process. Use this option when you have manually positioned the tape at the end of a backup sequence, or when you want to overwrite any data already on the tape.

Forward to End of Tape before starting copy?

Specify whether to forward to the end of the last image on the output

device before beginning this operation. This option would be used to stack multiple backups on to a single tape for example.

Device name for remote volume prompt

Specify this option when backing up to a remote or local server to indicate the name of a terminal device on which to display volume prompt messages for multi-volume operations.

3. Once you have entered your selections, press the Enter key to begin the process.

Chapter 18. Listing or Verifying Backups

This chapter describes the steps for listing or verifying the contents of a SysBack backup.

Listing Backup Contents

Use this option to list the contents of any SysBack backup. This option shows the header information for the backup, a list of the logical volumes or filesystems included (except on file/directory backups), and optionally a complete list of files and directories on the backup. This does not actually read the backup image to ensure that the files are actually present. This process reads the table of contents that was created during the backup preprocessing stage.

To list the contents of a backup:

1. At a command line, type `smit`.
2. From the SMIT menu, select **System Backup & Recovery for AIX**.
3. Select **Backup & Recovery Options**.
4. Select **List Backup Contents**.

Note: You can also access this menu using the fastpath. To do this, type `smit sb_list` at a command line.

5. On the Device Selector screen, highlight the device you want to use and press Enter.
6. The following screen is displayed. This screen shows the default options and values available when you list the contents of a backup to a local tape drive.

List Backup Contents

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

Hostname of server
Device or file name
Backup sequence number
Display file list?

[Entry Fields]
hambone.austin.ibm.com
/dev/rmt0
[1]
yes

+

F1=Help
F5=Reset
F9=Shell

F2=Refresh
F6=Command
F10=Exit

F3=Cancel
F7=Edit
Enter=Do

F4=List
F8=Image

Figure 18-1. Default Options and Values Available When Listing the Contents of a Backup from a Local Tape Drive

The fields have the following definitions:

Hostname of server

The server hostname if a server option was

selected on the prior device selector screen. You cannot change this field.

Device name

The device, if a tape drive or virtual device was selected. You cannot change this field from this screen.

Backup sequence number

Default=1. If the multiple backups were performed sequentially to the device, select the sequence number of the backup to list files for. This field is displayed only when you are listing the contents of a backup from a tape drive or virtual device.

Display file list?

Default=yes. To display the list of files on the backup in addition to the backup header information, select "yes." You can press Tab to change the value to "no." This field has no affect when you are listing the contents of a logical volume backup, because this backup does not contain individual files.

7. Press Enter when all fields are correct.

The system begins reading the tape. If you selected a backup sequence number other than "1," the tape first forwards past the prior backups before reading the backup information. The contents of the backup are displayed, along with a list of logical volumes and filesystems, and the optional list of files and directories on the backup.

The following is an example list of the backup header and images (filesystems and logical volumes) information:

Backup Header

```
-----
Date:   Sun Mar  9 13:48:02 1997
User:   root
Host:   sbclient
Type:   TOC - Volume Group
Data:   vg00
Size:   33 megabytes
Packed: N
Buffer: 64 Kbytes
Bkend:  B
Volume: 1
```

Images contained on this backup:

Image	VG name	LV Name	Size	Mount Point
1	vg00	lv02	1	/testfsnew
2	vg00	rawlv2	24	-
3	vg00	rawlv3	8	-

The list above indicates that this is a volume group backup of the vg00 volume group and includes "raw" logical volumes rawlv2 and rawlv3 and the /testfsnew filesystem.

Verifying Files on System Backup

It is often a good idea to verify all of the data on a backup to ensure that the backup was written properly. For backups containing multiple data options, such as multiple volume groups or multiple filesystems, you can verify all or part of the backup. For instance, if you created a system backup containing multiple volume groups, you can verify one volume group, multiple volume groups, or all volume groups on the backup. Likewise, for a logical volume backup containing multiple logical volumes, you can verify one or more logical volumes. This process actually reads the backup images and may provide a list of files that are actually contained on the backup media. You may use this listing to compare to the table of contents listing created by executing section “Listing Backup Contents” on page 18-1 to determine if discrepancies exist.

To verify data on a backup:

1. From the Backup & Recovery Options menu, select **Verify a Backup**.

Note: From a command line, type `smit sb_verify`.

2. On the Device Selector screen, highlight the device you want to use and press Enter.
3. If you selected a tape drive or virtual device, enter the backup sequence number. The default value is “1,” indicating that the backup to be verified is the first backup on the media. If you stacked multiple sequential backups on the media and want to verify a different backup, type the backup number and press Enter.
4. Next, the backup is read to determine the backup type. If the backup is not a file or directory backup, you are asked to select the data to be verified. A list of verify options appear, dependent on the backup type. For instance, if this is a volume group backup, the list includes volume groups to verify. If this is a filesystem backup, the list includes filesystems. To select a single option to verify, highlight the option and press Enter. To select multiple options, highlight each line and press F7. When all selections have been made, press Enter to continue.
5. The following screen shows the default options and values that appear when you verify the contents of a volume group backup of vg00 from a local tape drive:

Verify a Backup

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

	[Entry Fields]
Hostname of server	hambone.austin.ibm.com
Device name	/dev/rmt0
Verify data type	Volume_Group
Report output type	both +
Device name for remote volume prompt	[]
Data to verify (of above type)	[rootvg]

F1=Help
F5=Reset
F9=Shell

F2=Refresh
F6=Command
F10=Exit

F3=Cancel
F7=Edit
Enter=Do

F4=List
F8=Image

Figure 18-2. Default Options and Values Available When Verifying the Contents of a Volume Group Backup

The fields have the following definitions:

Hostname of server	The server hostname if a server option was selected on the prior device selector screen. You cannot change this field.
Device name	The device, if a tape drive or virtual device was selected. You cannot change this field from this screen.
Disk image file	The name of the disk image file previously selected. This field is displayed only if a disk image file name was selected. You cannot be change this field from this screen. device image file:verifying
Verify Data Type	The backup type. It indicates the type of data, as shown in the Data to verify field, that is to be verified. This field is for information only and cannot be changed.
Report output type	Default=progress indicator. Keep the default value if you want to display a progress indicator during the backup process, which indicates the approximate total backup time and amount completed. Press Tab to select "file list" to display a list of files as they are being backed up, or Tab once more to show "only errors" that occur during the backup.
Device name for remote volume prompt	Default=(Blank/None). Enter a TTY, LFT or PTS device name to send the volume prompt to a specified device rather than to the current SMIT screen. If you are backing up to a remote host, the device name you specify is attached to the

remote host. This field is displayed when the backup device is a tape drive or virtual device.

Examples of device names are `/dev/tty0`, `/dev/lft0` and `/dev/pts/5`. You can determine the terminal device name by typing `tty` at the command line on that device.

Data to verify (of above type) Unless the backup is a file/directory Backup, this field contains the data to verify as selected on the prior screen. This can be a list of volume groups, filesystem, or logical volumes, depending on the type of backup to be verified. For a file/directory backup, this field is left blank and any contents are ignored, because the entire contents of the backup must be verified.

6. Press Enter when all fields are correct.

Each data type specified is read in its entirety to ensure the data is readable on the media. Either a list of files or progress indicator is displayed during the verification as selected above.

Chapter 19. Activity Logging

The SysBack log file provides a mechanism to track the completion status of backup, restore, and verify operations. The log can be used in conjunction with the progress indicator or file list options, which are used to monitor the ongoing status of backup, restore, and verify operations.

The sysback log, implemented in a fixed size and in a circular manner, never grows beyond a specified size. This is called a “head and tail” log. As the log file grows, the head of the log approaches the tail as if it were a circle. When the head catches the tail, the log has reached its maximum size and the oldest entries in the log are purged to make room for new entries. The length of time SysBack log entries are held is directly related to the maximum size of the log. Increasing the log size enables the storage of entries for a longer period of time, chronologically.

You can change the default log size and location and also list the log entries.

Accessing the SysBack Logging Menus

To view the SysBack log entries:

1. From the SysBack Main Menu, select **Utilities**.
2. From the Utilities menu, select **SysBack Logging**.

Note: At a command line, type `smit sb_logging`.

Changing the SysBack Logging Attributes (Size and Location)

The SysBack log file (`sysback.log`) is located, by default, in the `/var/adm/ras/` directory. You can change this location, as well as the log size (4096 bytes or 4 Kbytes by default, the minimum size).

You can increase the log size in increments of 4 Kbytes, provided that there is sufficient space in the log’s destination directory. If you specify to increase the log size to a number that is not a 4 Kbyte increment, the log size is automatically set to the next largest multiple of 4 Kbytes. For example, if you specify a size of 4098, the size will be automatically set to 8192, because 4098 is not a multiple of 4 Kbytes.

To change or show the SysBack logging attributes:

1. From the SysBack Logging menu, select **Change/Show SysBack Logging Attributes**.

Note: At a command line, type `smit sb_changelog`.

2. The following screen is displayed:

Change/Show Sysback Attributes

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

Sysback Log Filename	[Entry fields] [/var/adm/ras/sysback.log]
Sysback Log Size	[8192]

F1=Help	F2=Refresh	F3=Cancel	F4=List
F5=Reset	F6=Command	F7=Edit	F8=Image
F9=Shell	F10=Exit	Enter=Do	

Figure 19-1. The Change/Show SysBack Logging Attributes Menu

The fields have the following definitions:

SysBack Log Filename (Required)

Specifies the fully-qualified path for the log location. The default location is **/var/adm/ras/sysback.log**.

Note: Renaming the log file does not remove the previous log name from the file system.

SysBack Log Size (Required)

Specifies the size, in 4096 bytes (4 Kbytes) increments, of the log. The default size is 4096.

Displaying the SysBack Log

Use the **Display SysBack Log** option to view the contents of the SysBack log.

To display the log, select **Display SysBack Log** from the SysBack Logging menu.

Note: At a command line, type `smit sb_displaylog`.

The following is an example of a SysBack log:

```
===== ALOG /var/adm/ras/sysback.log output =====
```

```
Command: /usr/sbin/mkdirback -f/usr/lpp/sysback/bf/local/all -I06261530
-x -p /home/jdavis/sample.txt
Date: Mon Jun 26 15:31:13 CDT 2000
File "/home/jdavis/sample.txt" does not exist or is not readable.
```

```
FAILURE: Files or Directory backup failed to complete.
```

```
Command: /usr/sbin/mkdirback -f/usr/lpp/sysback/bf/local/all -I06261534 -x
-p /home/jdavis/.profile
Date: Mon Jun26 15:34:48 CDT 2000
Backup up files '/home/jdavis/.profile'
Start date is Mon Jun 26 15:34:49 CDT 2000
User is root at
Estimated size is 1 MB
```

```
SUCCESS: File/Directory backup completed successfully.
```

```
===== ALOG /var/adm/ras/sysback.log output =====
```


The format of the log entry is described below:

Command

The backup, restore, or verify command syntax executed.

Date The date and time that the backup, restore, or verify command syntax executed.

Error Information

The last fatal error that caused an error in the backup, restore, or verify command.

Status Described as SUCCESS, WARNING or FAILURE, indicating that the operation completed or failed.

Chapter 20. Scheduled Backups and Scripts

The SysBack Scripts and Scheduling functions provide a mechanism to automate common backup functions that require little or no user interaction. The SysBack Scripts functions help you build command syntax into a Korn Shell script that can be scheduled with SysBack. The SysBack Scheduling functions enable you to take these scripts and schedule them to run automatically at a specified time or interval. The Scheduling functions act as a front-end to crontab and enables you to add, update, and remove SysBack backup scripts to crontab.

Scripts

Accessing the Backup Scripts Menu

The Backup Scripts menus enable you to create, change, or remove backup scripts.

To access the Backup Scripts menus:

1. From the SysBack Main Menu, select **Backup Schedules and Scripts**.

Note: At a command line, type `smit sb_script_sched`.

2. Select **Backup Scripts**.

Note: At a command line, type `smit sb_script`.

Creating a Backup Script File

When you create the backup script file, the SMIT options with which you are presented give the appearance that a backup will be performed. These options are only used to create the backup command sequence, and not to start a backup.

The scripts create with the **Create a Backup Script File** option are stored in the `/usr/lpp/sysback/sbscripts` directory, unless a fully qualified path name is specified in the script name field.

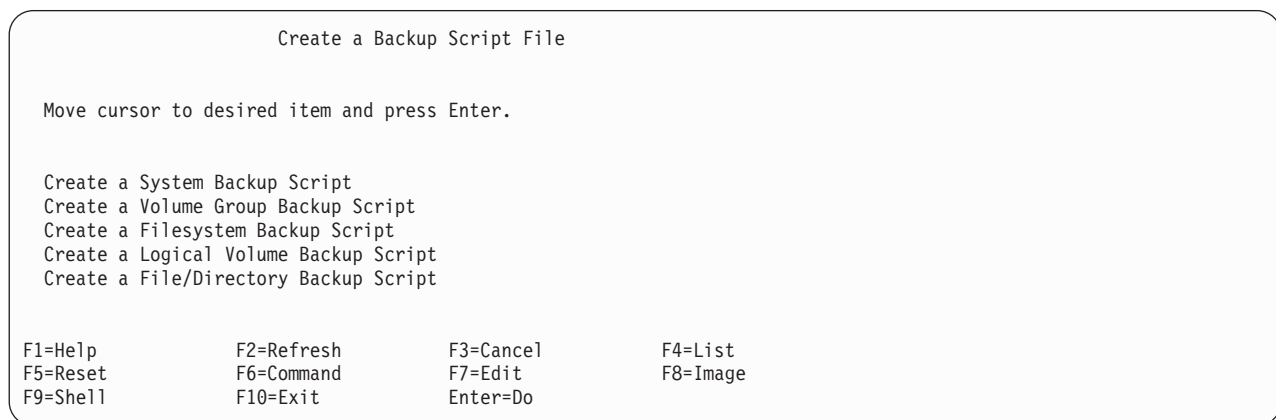


Figure 20-1. Create a Backup Script File Menu Options

To create a backup script file:

1. From the Backup Scripts Menu, select **Create a Backup Script**.

Note: At a command line, type `smit sb_script_c`.

2. Select the type of backup script you want to create. The following choices are available:
 - **Create a System Backup Script**
 - **Create a Volume Group Backup Script**
 - **Create a Filesystem Backup Script**
 - **Create a Logical Volume Backup Script**
 - **Create a File/Directory Backup Script**

Note: For this example, **Create a System Backup Script** is used.

3. On the Device Selector screen, highlight the device you want to use and press Enter.
4. The following screen is displayed.

Create a System Backup Script

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

[TOP]

Backup Script Name	[system_backup]
Description	[System Backup]
Overwrite Existing Script	No
Save Backup Output to a Log?	No
Location of Log File	[]
Overwrite Previous Log?	No
HOSTNAME of server	
Device Name	[/dev/rmt0]
Create a Power Backup?	No
Report output type	File List
Platform/kernel type for tape boot image	rsbc/MP
Network install support to include	
Compress data before writing to media?	No
User Description	[]
Buffer size (in Kbytes)	[64]
Preserve Physical partition mapping?	No
Device name for remote volume prompt	[]

F1=Help

F5=Reset

F9=Shell

F2=Refresh

F6=Command

F10=Exit

F3=Cancel

F7=Edit

Enter=Do

F4=List

F8=Image

Figure 20-2. The Create a System Backup Script Menu

The first three options are described below. The other options are identical to the options available when you create a system backup. For descriptions of those options, see the instructions for creating system backups in Chapter 4, “Performing Backups”, on page 4-1.

The first six options have the following definitions:

Backup Script Name (Required)

The fully-qualified filename for the backup script. If a directory is not specified, the script is created in the `/usr/lpp/sysback/sbscripts` directory by default.

Description (Optional)

The purpose or content of the script. If no description is provided, the description, by default, reflects the type of backup performed by the script.

You can use any character or number, except for single (') or double (") quotation marks.

Overwrite Existing Script (Optional)

Determines whether or not to overwrite an existing backup script. The default is "No"

Save Backup Output to a Log?

Indicates to save backup output to a log by redirecting stdout and stderr.

Location of Log File

Specify the fully qualified path and filename to be used as the backup log file. If this option is not specified when the **Save Backup Output to a Log?** option is set to yes, this value will be defaulted such that the log filename created is based on the date and time that the backup is run. If a file is automatically created by SysBack, it will be created in the directory: **/usr/lpp/sysback/log** and will be in the form of:
`sysback$(date "+%m%d%H%M")`

where the variable string will be expanded to the current date and time when the file is created.

Overwrite Previous Log?

Specify this option to overwrite a previously created log filename. For example: Perhaps you have MON, TUE, WED, THU, and FRI backup logs/scripts. Each Monday, you would like for the existing MON script to overwrite the MON log from the previous week. This option will execute this action.

5. Press Enter to confirm your selections.

The following file is an example of a backup script generated using the options specified above.

```
#!/bin/ksh
# Command filename: /usr/lpp/sysback/scripts/system_backup
# Description: System Backup

sysback -v -f /dev/rmt0 -T rspc -k mp

exit $?
```

Note: The commands contained in the backup script file are not checked for validity. Always verify the validity of the backup script by performing a backup using the same options as those in the backup script.

Changing a Backup Script File

Use the **Change a Backup Script File** option to edit the contents of a backup script created by SysBack. You can add additional commands or change the existing commands and options.

The **Change a Backup Script File** option uses the AIX vi editor and provides help screens and pre-programmed function keys. However, you can edit the script file with any text editor.

To change a backup script file:

1. From the Backup Scripts menu, select **Change a Backup Script File**.

Note: At a command line, type `smit sb_script_change`.

2. Select the script file you want to edit and press Enter.
3. The following vi help screen is displayed. This screen lists the actions you can perform, as well as the corresponding function key or key sequences.

EDITOR HELP SCREEN		
You are about to enter the "vi" editor. If your terminal type provides function keys, the following function keys may be used for editing the file. The standard "vi" commands shown may also be used if function keys are not provided.		
FUNCT KEY	ACTION	STANDARD VI KEY
F1	Display this help screen	:e#
F2	Exit without saving changes	:q!
F3	Save changes and exit	:wq!
F4	Page Back	CTRL-B
F5	Page Forward	CTRL-F
F6	Begin/End Insert Mode	i/ESC
F7	Insert Line (F6 to quit)	o/ESC
F8	Delete Character	x
F9	Delete Line	dd
=== Press F1 or ":e#" to edit file ===		

Figure 20-3. The vi Editor Help Screen

Notes:

- a. Press F1 at any time to return to the help screen.
 - b. Press F2 at any time to exit the editor without saving the changes.
4. Press F1 to exit the help screen and begin editing the file.

Removing a Backup Script File

Use the **Remove a Backup Script File** option to remove existing SysBack script files.

To remove a backup script file:

1. From the Backup Scripts menu, select **Remove a Backup Script File**.

Note: At a command line, type `smit sb_script_remove`.

2. Select the script file you want to edit and press Enter.
3. Press Enter to confirm the removal of the script file.

Accessing the Backup Schedules Menus

The Backup Schedules menus enable you to create, update, list, and remove backup schedules.

To access the backup schedules menus:

1. From the SysBack Main Menu, select **Backup Schedules and Scripts**.

Note: At a command line, type `smit sb_script_sched`.

2. Select **Backup Schedules**.

Note: At a command line, type `smit sb_sched`.

Creating a Backup Schedule

Use the **Create a Backup Schedule** option to schedule an existing backup script. This script can be one created by SysBack or a user-defined script.

The **Create a Backup Schedule** option provides a front-end to the AIX **crontab** and features a menu-based method for creating a schedule.

To create a backup schedule:

1. From the Backup Schedules menu, select **Create a Backup Schedule**.

Note: At a command line, type `smit sb_sched_c`.

2. The following screen is displayed:

Create a Backup Schedule

Type or select values in entry fields
Press Enter AFTER making all desired changes.

Script Name

[/usr/lpp/sysback/scripts/system_backup

Schedule ID

Schedule Description

[Friday and Wednesday Full System Backup]

Minute (0-59)

[0]

Hour (0-23)

[23]

Day (1-31)

Month (1-12)

Week Day (0-6)

[3,5]

F1=Help

F2=Refresh

F3=Cancel

F4=List

F5=Reset

F6=Command

F7=Edit

F8=Image

F9=Shell

F10=Exit

Enter=Do

Figure 20-4. The Create a Backup Schedule Menu

The fields have the following definitions:

Script Name (Required)

The name of an existing script file. Press F4 for a list of script files, or type the fully qualified path and file of the script file you want to use.

Schedule ID (No Input)

The Schedule ID is generated at command execution and is related to the schedule. You cannot enter any information in this field.

Schedule Description (Optional)

A description of the backup schedule. You can enter any text except single (') or double (") quotation marks.

Minute (Required)

Specifies the starting minute, a number between 0 and 59. Press F4 for a list of valid values.

Hour (Required)

Specifies the starting hour, in military time. Use a number between 0 and 23, where 0 equals 12:00 AM and 23 equals 11:00 PM.

Day (optional)

Specifies the day of the month, a number between 1 and 31. Press F4 for a list of valid values. If both this field and the WeekDay field are left blank, the schedule runs every day.

Month (optional)

Specifies the starting month, a number between 1 and 12. Press F4 for a list of valid values. If this field is left blank, the schedule runs every month.

WeekDay (optional)

Specifies the day of the week, a number between 0 and 6, where 0 equals Sunday. Press F4 for a list of valid values. If both this field and the Day field are left blank, the schedule runs every day.

Important Field Input Notes:

- a. Two numbers separated with a dash indicate an inclusive range. For example, to schedule a command to run Tuesday through Friday, type "2-5" in the WeekDay field.
 - b. Numbers separated with commas indicate that the schedule should run on separate days. For example, to run a schedule on the first and last days of January, type "1" in the Month field and "1,31" in the Day field.
3. Press Enter to commit the selections.

Note: Do not make changes to the schedule through manual manipulation of **crontab**. Because SysBack acts as a front-end to **crontab**, making changes manually causes the SysBack scheduling features and **crontab** to be unsynchronized.

Updating a Backup Schedule

To update an existing backup schedule that was created by SysBack:

1. From the Backup Schedules menu, select **Update a Backup Schedule**.

Note: At a command line, type `smit sb_sched_u`.

2. Select the schedule you want to update and press Enter.
3. The following screen is displayed:

Change or Update an Existing Backup Schedule

Type or select values in entry fields
Press Enter AFTER making all desired changes.

Script Name	[/usr/lpp/sysback/scripts/system_backup]		
Schedule ID	SB1		
Schedule Description	[Friday and Wednesday Full System Backup]		
Minute (0-59)	[0]		
Hour (0-23)	[23]		
Day (1-31)	[]		
Month (1-12)	[]		
Week Day (0-6)	[3,5]		

F1=Help	F2=Refresh	F3=Cancel	F4=List
F5=Reset	F6=Command	F7=Edit	F8=Image
F9=Shell	F10=Exit	Enter=Do	

Figure 20-5. The Change or Update an Existing Backup Schedule Menu

For descriptions of the above options, see "Creating a Backup Schedule" on page 20-5.

4. Press Enter to commit the changes.

Listing Backup Schedules

To list existing backup schedules created by SysBack, select **List Backup Schedules** from the Backup Schedules menu.

Note: From a command line, type `smit sb_sched_l`.
The following is an example of the output produced.

Command: /usr/lpp/sysback/sbscripts/file.lasher.2

ID: SB1

Description: Sample Test Schedule for host lasher

Execution Time:

Every: 15th in the month(s) of June at 9:25 a.m.

Removing a Backup Schedule

To remove an existing backup schedule:

1. From the Backup Schedules menu, select **Remove a Backup Schedule**.

Note: At a command line, type `smit sb_sched_r`.

2. Select the schedule you want to remove and press Enter.
3. Press Enter again to confirm the removal of the backup schedule.

Note: Removing the backup schedule in this manner removes the schedule from SysBack, as well as its corresponding entry in **crontab**.

Chapter 21. Virtual Devices

A virtual device enables you to logically group multiple physical devices into a single “virtual” device for easier reference. For example, if you want to use three tape drives in parallel to perform your backups, you can configure those drives into a virtual device description. Therefore, each time you want to backup or restore from those parallel devices, you need to specify only the virtual device name.

Note that any tape drive can be configured into one or more virtual devices. For instance, the same tape drive used in a list of sequential virtual devices can also be used in a list of parallel virtual devices.

Note: When configuring multiple physical devices into a single virtual device, you can use tape drives of different types. The only limitation is that all drives must be configured to the same block size. When you use a parallel or multi-copy virtual device, the speed of the backup is limited to the speed of the slowest device.

To access the SysBack menus for managing the virtual devices:

1. At a command line, type `smit`.
2. Select **System Backup & Recovery for AIX**.
3. Select **Configuration Options**.
4. Select **Virtual Devices**.

You can also access these menus using the fastpath. To do this, type `smit sb_virdev` at a command line.

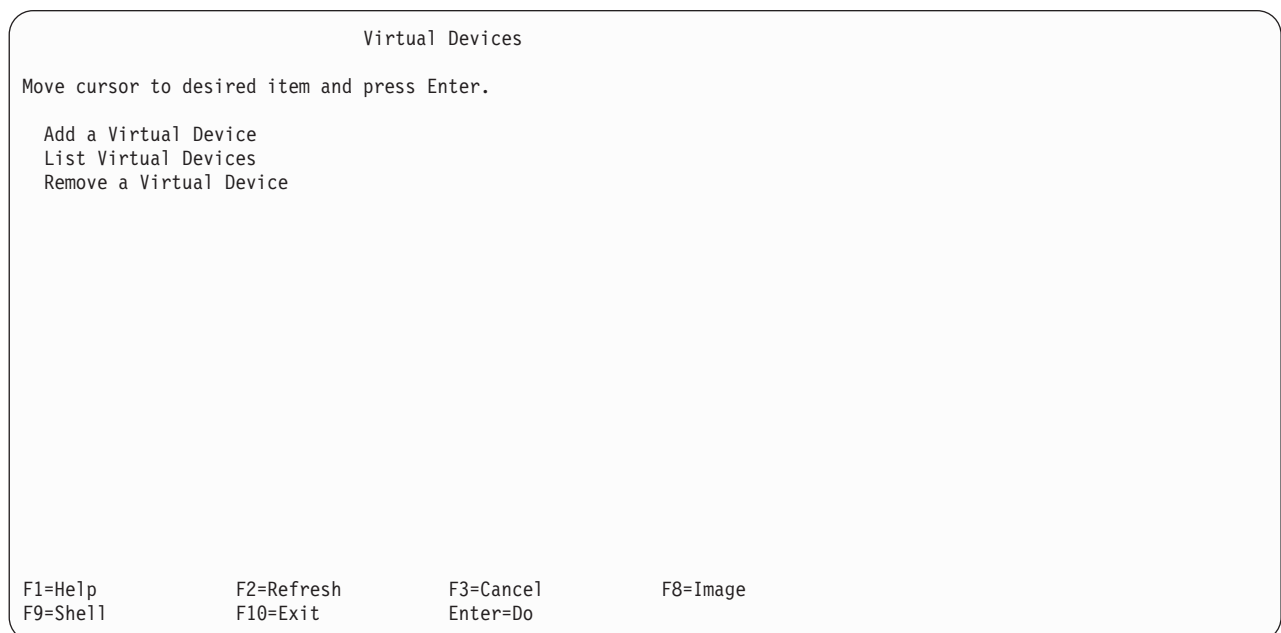


Figure 21-1. The Virtual Devices Menu

Types of Virtual Devices

SysBack uses the following types of virtual devices:

Sequential A group of devices that are used sequentially, meaning that when one device reaches its capacity, the backup or restore automatically continues on the next device in the list. You can have up to eight sequential devices in the list. When the last device in the list reaches its capacity, the user is prompted to change the media in all of the devices before the backup can continue.

Parallel A group of devices that are used in parallel. In this case, the data is “striped” across all of the drives in the list, meaning that the first cluster of data is written to the first drive, the second to the next drive, and so forth. The writes are optimized to keep as many drives as possible streaming at all times for best performance.

Although you can back up in parallel to eight drives at a time, using more than three drives often exceeds the read performance of the disk drive you are reading from. After you have exceeded the read performance during a backup, there is no benefit to having additional parallel devices. In fact, when the writes out-perform the reads, tape drives might no longer continue streaming and might enter a “start-stop” mode, decreasing the write performance even more. Finding the optimal number of parallel devices to use for your backups is a matter of trial and error. If performance decreases after adding an additional device to the parallel virtual device, you have likely exceeded the read performance of your disk drive or filesystem.

Note: Always keep in mind when using parallel devices that you must have the same number of devices available in order to list or restore the files from the backup.

Multi-Copy A group of devices that each receive an identical copy of the data being backed up. Unlike parallel devices, this virtual device type results in identical copies of the same data. This is useful for creating multiple backups at one time, either for replicating systems or for both on-site and off-site storage of backup tapes. Multi-copy backups often take little more time than a single backup, because only one copy of the data is being read. Performance has been optimized to enable several devices to be written to without decreasing performance. Again, finding the optimal number of devices without severely impacting overall backup performance is a matter of trial and error.

Note that each copy created using a multi-copy virtual device is equivalent to a single sequential backup. Therefore, each of the backups created with the multi-copy virtual device can only be read independently using a single tape device name or a sequential virtual device name.

Volume Numbering

When a device reaches the end of the media, the volume number is changed and a new volume header is written to the next volume. How the volume number is incremented differs from one virtual device type to another:

Sequential The volume number is always incremented by one. When the first

device reaches the end of media, the backup continues on the next device (volume two). When the last device in the list reaches the end of volume, the user is prompted to change the volume in *all* of the drives before the backup can continue. It is necessary to change volumes in all drives even if only one of the drives will be used before the backup completes.

- | | |
|-------------------|--|
| Parallel | The volume number of the first drive begins with A1, the second drive, B1, and the third, C1. When any of the drives reaches end of volume, the second digit is incremented by one. For instance, if the second drive (B) reaches the end of volume, the next volume inserted in that drive will be B2. In this way, it is easy to determine which tapes belong with which drives and in what order. |
| Multi-Copy | The volume number in each drive always starts at one, and each is always incremented by one. Since the same data is written to all drives, all volume numbers will also be the same. Note, however, that all drives might not reach end of volume at the same time. Therefore, the only difference between the backups in each drive might be the amount of data on each volume. |

Below is an illustration to depict how the backup moves across tapes for each virtual device type:

Autoloaders

You can define any of the virtual device types as a tape library (or “autoloader”). By setting a virtual device to **autoloader/auto-eject**, any time a backup tape reaches end of media, the tape automatically ejects from the tape drive (if the tape drive supports auto-eject). If the tape drive has an auto-loader device, the autoloader senses that the tape has been ejected and automatically removes the tape cartridge and inserts the next available cartridge. When SysBack senses a new cartridge has been inserted, the backup continues automatically.

Note that the autoloader is defined for use in sequential mode only. Most autoloaders support sequential insertion of the tape cartridges. SysBack does not support random insertion of backup cartridges, but ejects the cartridge and waits for the autoloader to insert the next sequential cartridge.

You can use multiple autoloaders in conjunction with any of the virtual device types described above. Also, some autoloaders have multiple tape drives. When you use two drives in the same autoloader, the loader must be able to monitor both drives simultaneously and change the tapes in both drives as needed.

Adding a Virtual Device

Creating a virtual device is a matter of selecting one or more physical devices and selecting the type of virtual device to define.

To create a new virtual device:

1. From the Virtual Devices menu, select **Add a Virtual Device**.

Note: From a command line, type `smit sb_mkvrdev`.

The following screen is displayed:

Add a Virtual Device

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

	[Entry Fields]	
* Write Policy	Sequential	+
Description	<input type="text"/>	
Auto-loader/Auto-eject?	no	+
* Device name(s)	[/dev/rmt0 /dev/rmt1]	+

F1=Help
F5=Reset
F9=Shell

F2=Refresh
F6=Command
F10=Exit

F3=Cancel
F7=Edit
Enter=Do

F4=List
F8=Image

Figure 21-2. The Add a Virtual Device Menu

- You can change the following fields from the screen above:

Write policy

Default=Sequential. Press Tab to select either “Parallel” or “Multi-copy” write policy. You can also press F4 to list the three options and select from the list.

Description

Default=Blank. Although this field is left blank at this time, a generic description is provided if you do not enter a description. The default description depends on the write policy:

Sequential Sequential Virtual Device

Parallel Parallel Virtual Device

Multi-copy Multi-copy Virtual Device

Enter a description to override the description above. You do not need to include the physical device name in the description. Do not use single (') or double (") quotation marks in this field.

Autoloader/Auto-eject?

Default=no. Press Tab for “yes” if this device, or these devices, are autoloaders. If you set this field to autoloader, the user does not receive prompts to change the volumes.

Device name(s)

Default=Blank. Enter the device names to include in the list (preceded by /dev), or press F4 to list the available tape drives and select the drives using F7. If this device is an autoloader, you can enter only one device name.

If the write-policy is set to Parallel or Multi-copy, you must enter more than one device name in this field. If the write-policy is sequential, entering only one device name treats this device no differently than a single tape drive, unless you also indicate that the device is an autoloader.

3. Press Enter to create the virtual device.

The new virtual device name is generated and displayed on the screen. Repeat the above steps for each additional virtual device you want to add.

Listing Virtual Devices

To list all of the virtual devices currently defined, select **List Virtual Devices** from the Virtual Devices menu.

This list shows the virtual device name, whether the virtual device is configured as an autoloader or auto-eject device, the write policy (s=sequential, p=parallel, c=multi-copy), the virtual device description, and a list of the physical devices that make up the virtual device.

Removing a Virtual Device

To remove a virtual device:

1. From the Virtual Devices menu, select **Remove a Virtual Device**.

Note: From a command line, type `smit sb_remexclude`.

2. Enter the virtual device name to delete or press F4 to list the available virtual devices and select from the list.
3. Press Enter to delete the specified virtual device.

Chapter 22. Tape Drives

This chapter contains information on performing various functions on tape drives. For virtual devices, some functions can be performed for all physical tape drives defined for the virtual device. Most of these tape drive options can be performed from other AIX system administration SMIT menus, but are provided within SysBack.

To access the tape drive menus:

1. At a command line, type `smit`.
2. From the SMIT menu, select **System Backup & Recovery for AIX**.
3. Select **Tape Drive Options**.

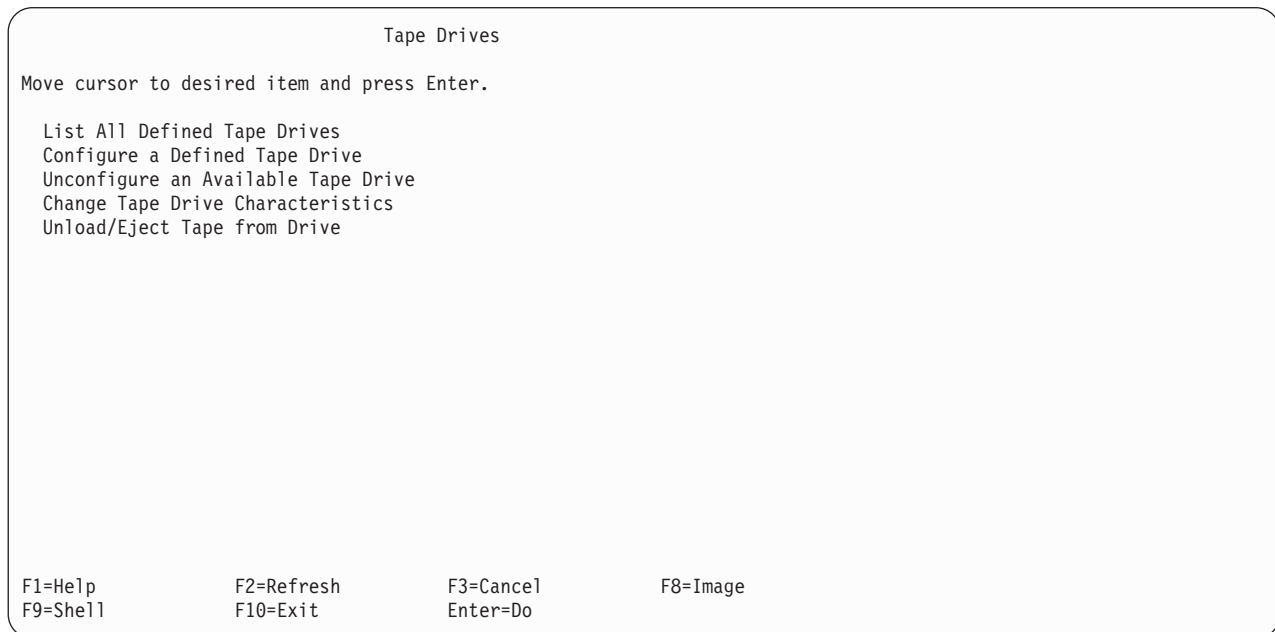


Figure 22-1. The Tape Drives menu

Listing tape drives

To list all tape drives defined to the system, whether currently available or not, select **List All Defined Tape Drives** from the Tape Drive Options menu.

The list includes all drives defined or available on the system. Only physical tape drives, and not virtual devices, are displayed. The drives labelled "Defined" have at one time been detected by the system but are currently unavailable, either because they are turned off, disconnected, or the **Unconfigure an Available Tape Drive** option was used against them. Devices labelled "Available" are available to use.

Configuring a defined tape drive

When a tape drive is either just turned on, reattached, or previously made unavailable, use this option to make the drive available for use.

To configure a defined tape drive:

1. From the Tape Drive Options menu, select **Configure a Defined Tape Drive**.
2. From the list of defined tape drives, select the drive you want to configure and press Enter.

If an error occurs, then the system is unable to detect the drive that it had previously defined. Make sure the tape drive is turned on and properly connected.

Unconfiguring an Available Tape Drive

You can make a tape drive unavailable for use by the system but still retain its definition in the system. To make a drive unavailable for use:

1. From the Tape Drive Options menu, select **Unconfigure a Defined Tape Drive**.
2. From the list of available tape drives, select the drive you want to unconfigure and press Enter.

Changing Tape Drive Characteristics

The characteristics of a tape drive that you can change differ from one drive type to another. One characteristic that is common to all drives is the **block size**. Refer to your tape drive documentation or the SMIT HELP screen (F1) for information on additional characteristics that can be changed.

To change the block size of a tape drive:

1. From the Tape Drive Options menu, select **Change Tape Drive Characteristics**.
2. From the list of available tape drives, select the drive whose characteristics you want to change.
3. A screen similar to the following is displayed:

Change / Show Characteristics of a Tape Drive

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

	[Entry Fields]	
Tape Drive	rmt0	
Tape Drive type	8mm5gb	
Tape Drive interface	scsi	
Description	5.0 GB 8mm Tape Drive	
Status	Available	
Location	04-C0-00-5,0	
Parent adapter	scsi0	
Connection address	5,0	
BLOCK size (0=variable length)	[1024]	+#
Use DEVICE BUFFERS during writes	yes	+
RETURN error on tape change or reset	no	+
Use EXTENDED file marks	yes	+
DENSITY setting #1	140	+
DENSITY setting #2	20	+
Use data COMPRESSION	yes	+

F1=Help

F2=Refresh

F3=Cancel

F4=List

F5=Reset

F6=Command

F7=Edit

F8=Image

F9=Shell

F10=Exit

Enter=Do

Figure 22-2. The Change/Show Characteristics of a Tape Drive menu

Depending on the type of tape drive, the options might differ from those above.

To change the block size, enter a new block size in the **BLOCK size (0=variable length)** field or press F4 for a list of valid entries.

Different tape drives might provide multiple block sizes for reading or writing the data. Use the same block size to read a tape that used to originally write the tape. It is generally more efficient to write tapes using larger block sizes (such as 1024, 2048) because this will usually increase the speed at which the data is written to the tape. It also usually increases the capacity of the tape because fewer “inter-block gaps” are needed between blocks written.

Notes:

- Only the root user has permission to change the block size of a tape drive.
- When you create a system backup, the tape block size is temporarily changed to 512-bytes, because the installation process that reads that tape is only capable of reading the tape at 512-byte blocks.

Refer to Appendix E, “Device/System-Specific Information”, on page E-1 for information on recommended tape drive characteristics.

- Press Enter to change the tape drive characteristics.

Unloading or Ejecting a Tape from the Drive

You can rewind and eject the tape cartridge from either a local or remote tape drive or virtual device, assuming the device supports auto-eject. If you select a virtual device, the tape is ejected from all physical devices defined for the virtual device. Whether the drive supports auto-eject or not, the drive door must be closed again (or opened and closed) before the drive can be used again.

To eject the tape from a drive or virtual device:

- From the Tape Drive Options menu, select **Unload/Eject Tape from Drive**.

2. From the list of tape drives and virtual devices available to both the local and remote systems, select the device you want to eject and press Enter.

Appendix A. Commands

cfgremrootaccess

Purpose

Adds, removes, or lists commands enables for Remote Command Access.

Syntax

```
➤—cfgremrootaccess—-h—"host"—➤
    |
    |--d—"host"—
    |--l
    |--c—"command"—
    --r
```

Description

The **cfgremrootaccess** command is used to configure a backup client to allow a server to remotely initiate its backups. This is called a “pull backup.” For example, A server contacts a client to start the backup; in response the client initiates the backup and sends the data to the server. Therefore, the server is actually “pulling” the backup operation from the client.

Using pull backups enables you to centrally manage your backups by initiating and controlling backup operations from a single location. You can further automate this central management of backups using the SysBack Scheduling and Scripting functions described in Chapter 20, “Scheduled Backups and Scripts”, on page 20-1.

Pull backups require not only Remote Services Configuration, but also Remote Command Access configuration. The Remote Services Configuration enables data to be sent across the network to the backup server. The Remote Command Access enables the server to initiate the pull backup.

Also note that the server that initiates the pull backup can be a different server than where the data is sent. Because of this, Remote Services can be configured between machine A, the client, and machine B, the backup server receiving the backup, while Remote Command Access is configured between machine A, the client, and machine C, the backup initiation server.

Flags

- c “command”**
Specifies the fully-qualified path and name of a command to allow for remote access. Used with the **-h** and **-r** flags.
- d “host”**
Specifies the hostname of a machine that is not allowed to contact the client to initiate a backup. Used only when the **-h** flag is set to “ALL”.
- h “host”**
Specifies the hostname of a machine that will initiate a backup of this client. This flag is required and must be used with the **-c** flag.
- l** Lists all commands enabled for Remote Command Access.
- r** Indicates to remove the command specified with the **-c** flag.

Examples

1. To allow the server sysback1.aix.dfw.ibm.com to contact this client to initiate a pull backup using the **/usr/sbin/sysback** command, type:

```
cfgremrootaccess -c '/usr/sbin/sysback' -h 'sysback1.aix.dfw.ibm.com'
```
2. To list all commands that are enabled for Remote Command Access and their respective hosts, type:

```
cfgremrootaccess -l
```
3. To remove the access for the **/usr/sbin/mkdirback** command, to be remotely initiated, type:

```
cfgremrootaccess -r -c '/usr/sbin/mkdirback'
```

Files

/usr/lpp/sysback/.root_access Lists commands and respective hosts allowed Remote Command Access.

Related Information

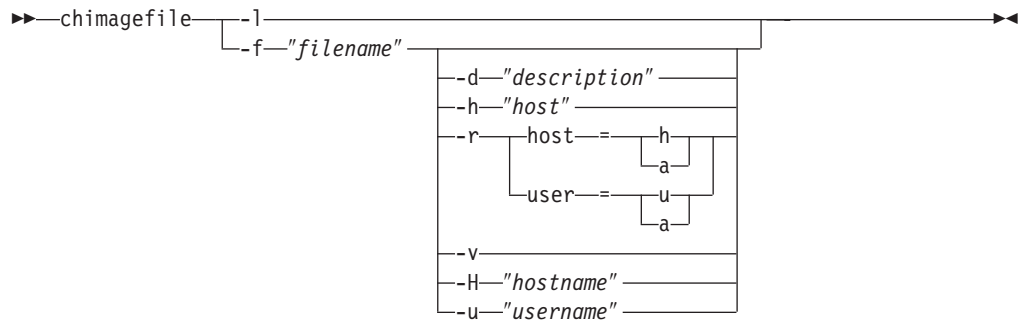
The **cfgremsvs** command.

chimagefile

Purpose

Changes the permissions of an existing disk image backup file.

Syntax



Description

When you perform a backup to a disk image file, you can set the read permission of the file to allow only the original host or original user to read from the file. You can change this permission at a later time if, for instance, you need to use an image file with “original host only” permission needs as a network installation image for other systems.

Using the **chimagefile** command, you can change the owner of the file (host or user), the backup description, or the host or user read permission of an existing image file.

Only the following users can change the read permission of a disk image file:

- Root user on the system where the file physically resides
- Root user on the system from which the file originated
- User who originally wrote the file

A file can only be accessed by the root user or by the same user who created the file if the file is in a directory the user has permission to access as defined by the **cfglocalaccess** or **cfgremaccess** commands. Only the root user can read backup image files contained in directories not explicitly defined.

Flags

-d “description”

Changes the user-defined backup description to the specified string. This description can be up to 60 characters. A longer string will be truncated to 60 characters. The description must be within double quotation marks (") and cannot contain single or double quotation marks.

-f “filename”

Changes the filename.

-h “host”

Changes the filename on the specified host.

-l Lists the current values, separated by colons (:), in the following order:

host_owner:user_owner:host_perm:user_perm:description

This flag is normally used only by SMIT for querying the current values.

-r host="[h/a]"

Changes the host read permission to the specified value. The possible values are *h*, indicating that only the host that owns the file can read it, or *a*, indicating that any host can read the file. The root user on the server where the file physically resides can also access the file.

-r user="[u/a]"

Changes the user read permission to the specified value. The possible values are *u*, indicating that only the user that owns the file can read it, or *a*, indicating that any user can read the file. The root user on the server or the root user on the host that owns the file can also access the file. Note that if any host is allowed to access the file, but only the user that owns the file can read it, the user who owns the file can access it from any host.

-v

Report the old and new values when they change. Without this flag, there is no output from this command.

-H "hostname"

Changes the current owner of the file to host *hostname*. Note that, if the host read permissions are currently set to *this host only*, changing the owner of the file to a new host prevents the original host from accessing the file. The root user on the server where the file physically resides can always access the file.

-U "username"

Changes the current user owner of the file to *username*. Note that, if the current user permission is set to *this user only*, changing the owner of the file to a new user will prevent the original user from accessing the file. The root user on the host that owns the file, or the root user on the server in which the file physically resides will always be able to access the file.

Examples

1. To change the image file `/usr/lpp/sysback/bf/pluto/root/plutoV.220934` to allow *all* users on all hosts to read this file, type:

```
chimagefile -r host=a -r user=a -f \  
/usr/lpp/sysback/bf/pluto/root/plutoV.10220934
```

2. To change the current host of the file `/usr/lpp/sysback/images/anyhost.udevrg.043141022` to host *mercury*, and the backup description to master udevrg volume group, assuming the file exists on the server *mars*, type:

```
chimagefile -d "master udevrg volume group" -H mercury \  
-h mars -f \  
/usr/lpp/sysback/images/anyhost.udevrg.043141022
```

Related Information

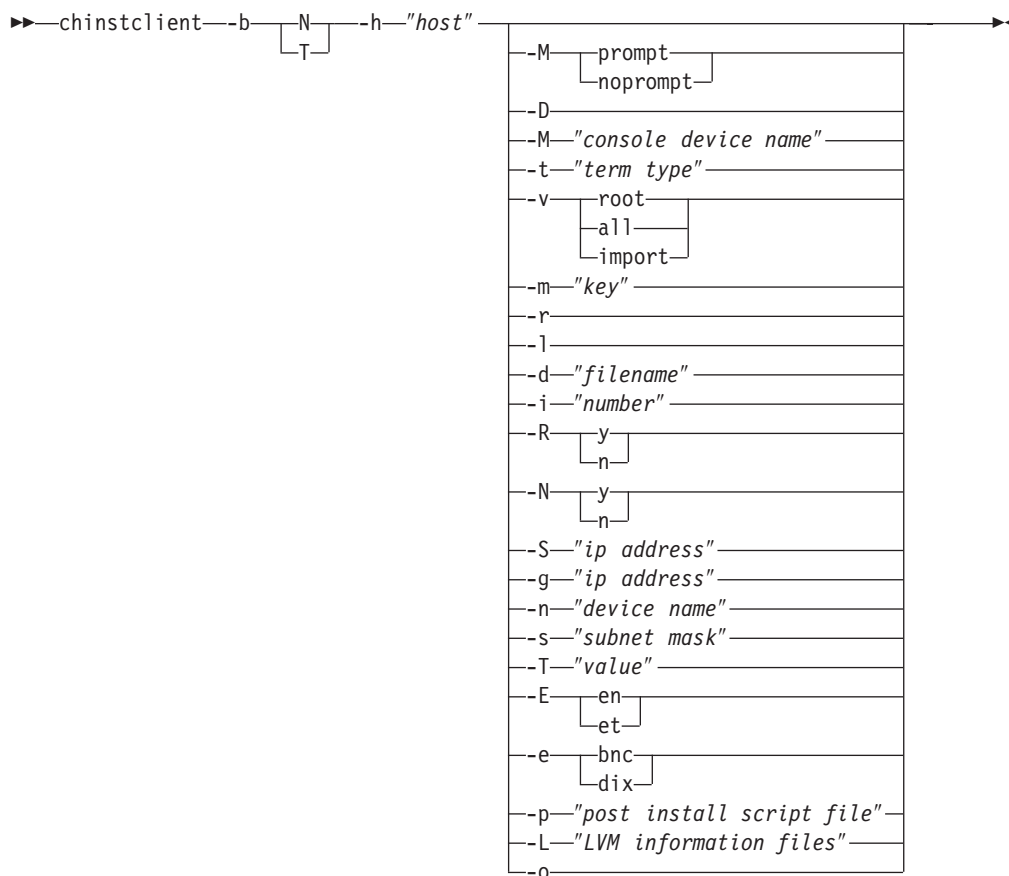
The `cfglocalaccess` and `cfgremaccess` commands.

chinstclient

Purpose

Sets client defaults for use during a tape or network boot/installation process.

Syntax



Description

The **chinstclient** command enables you to specify response to common prompts during a boot and installation process. Setting these defaults can minimize, and in some cases eliminate, the need for user prompting during a boot and installation process.

These defaults are set on a client-by-client basis.

Flags

-b "N | T"

Specifies if the defaults are for a tape or network boot and installation process.

-h "host"

Specifies the name of the client.

-M "prompt | noprompt"

Specifies whether or not to prompt the client. If this field is set to "noprompt",

the installation menus appear after a network boot. Otherwise, the installation occurs after the network boot without prompting the user, as long as all required information for the user is also provided.

-D

Turns on debug logging operations for troubleshooting network boot and installation problems.

-c "console device name"

To prevent the prompt before installation that determines the console to be used for installation, enter the name of the console here. The console can be either an LFT (graphical display) or TTY (ascii display) device. Examples are `"/dev/lft0"` or `"/dev/tty0"`. If an LFT device exists on the client, you can select it by typing `/dev/console`.

Note: You must select a display, even for no-prompt installations, in order to receive error or warning messages and to enable prompts if the default information provided is insufficient.

-t "term type"

If you specified a TTY device, specify a terminal type. This ensure that the installation menus, if required, display with the correct terminal emulation. Examples of common terminal types are `"ibm3151"`, `"tvi925"`, and `"vt100"`.

-v "root | all | import"

Specifies how to handle volume group processing during installation. The available options are:

Recreate and restore rootvg only

Only the rootvg volume group is created and restored from the media, even if other volume groups are defined on the backup. At the end of the installation, rootvg is the only defined volume group.

Recreate and restore all volume groups

All volume groups included on the backup media are created and restored. Volume groups defined on the original system but whose data was not included on the backup, are created but no data is restored.

Recreate and restore rootvg and import all other volume groups from disk

The rootvg volume group is created and restored and all other volume groups are imported from disks on the client. This options assumes that the non-rootvg volume groups already exist on the client. This option is typically used when restoring the rootvg volume group after a system failure where no other volume groups were affected.

-d "filename"

Specifies the name of the installation image file that contains the backup image to be used or an installation tape device. If you are installing from a file, the directory containing the file was configured using the `cfgremaccess` command and is the only directory path available for installation image files. Specify the file here to prevent being prompted for it during installation.

-i "number"

If the client is to be installed from tape and the system backup is not the first backup on the tape, enter the backup sequence number. This number must be between 1 and the total number of system backups on the tape.

-R "y | n"

Indicates whether or not to remove the SysBack program from the system after installation. Choose `"y"` for yes when you have not purchased a license for the client that will be installed. The default is `"n"` or no.

-N "y|n"

Indicates whether or not to remove network specific information required to configure the host to the network. This option is useful when the machine installed was cloned from a backup image of a machine that is still present on the network. The default is "n" or no.

Note: This option has no effect when cloning images between partitions of the same LPAR Capable machine.

-S "ip address"

The address of the installation server. If the backup media from which the client will be installed exists on a different server than the network boot server, enter the IP address of the installation server here.

-g "ip address"

The IP address of the gateway, if the client will be installed from a different server than the network boot server, and a different gateway address is required to reach the installation server.

-n "device name"

The network device name, if the client will be installed using a different network adapter than it was booted from. The name should be in the format of "entX", or "tok0".

-s "subnet mask"

The subnet mask required for the network adapter used to contact the installation server, if the client will be installed from a different network adapter than it was booted from.

-T "value"

The token ring speed of the network for network installations over a token ring interface. If the boot server is also the installation server, you do not need to set this option. If the installation server uses a different network adapter, and the network adapter is token ring, specify the correct token ring speed.

-E "en | et"

The ethernet interface used for network installations over an ethernet interface. If the boot server is also the installation server, you do not need to set this option. If the installation server uses a different network adapter, and the network adapter is ethernet, specify the correct interface.

-e "bnc | dix"

Specifies the ethernet connection type for network installation over an ethernet interface. If the boot server is also the installation server, you do not need to set this option. If the installation server uses a different network adapter, and the network adapter is ethernet, specify the correct connection.

-p "post install script file"

The fully-qualified path and name of a post-install script to run at the end of installation. The file must exist on the installation server and be readable by any user. For more information about post-install scripts, see Appendix D, "Creating Scripts for Customizing the System Backup and Install Process", on page D-1.

-L "LVM information file"

The fully-qualified path and name of an LVM information file. The LVM information file must contain information that is compatible with the client. The file must exist on the installation server and be readable by any user. For more information about LVM information files, see Chapter 16, "Utilities", on page 16-1.

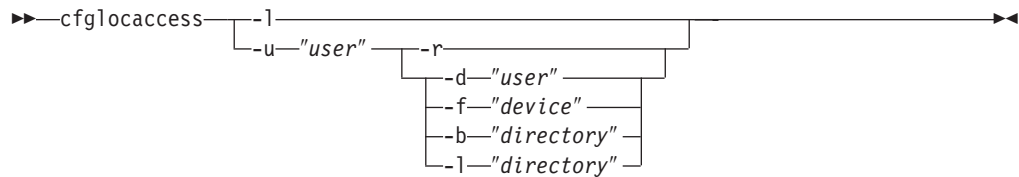
- o Overrides the **/etc/SDR_dest_info** file from the boot server. If a system backup image was created on an SP node from a different SP complex, the **/etc/SDR_dest_info** file will refer to the wrong control workstation, and post-installation customization will fail. Specifying this options causes the correct file to be copied from the boot server before the **pssp_script** post-install script runs.

cfglocaccess

Purpose

Adds, lists, or removes local user access to backup devices and directories.

Syntax



Description

All users on the system are provided access to all of the backup devices on the system when SysBack is first installed. This is accomplished by providing a permission record for a user called *all*. You might not want certain users to have access to all devices and backup directories, so you can deny specific users access or change the device or directory list that specific users are allowed to use. The devices and directories specified when using this option determine the list of backup options that users receive when they perform backups using SMIT, and those devices or directories that other SysBack commands, executed at the command line, are permitted to read or write to.

If you do not want all users on the system to have the same access, remove access to user *all*, using the `-r` flag, before setting up access to specific users.

SysBack provides flexibility in assigning users access to devices, directories, and so on. For instance, you can assign specific devices or directories to each user on the system or assign a device to all users on the system except specific users. Refer to “Adding or Changing Local User Device/Directory Access” on page 7-2 for details and examples of user permissions.

Flags

-b “directory”

Specifies one or more directories, separated by spaces, to which the user can perform regular backups. The user can back up to any subdirectory in the directories provided here. When performing any SysBack backup, the user has a disk image file backup option for each directory specified.

-d “user”

Specifies users, separated by spaces, that are to be explicitly denied access. If you use this flag when you are adding or changing a permission record for *all* users, all users *except* those specified will be permitted.

-l Lists current user permissions.

-f “device”

Specifies a list of tape drives or virtual devices, separated by spaces, to which the user or users can perform backups. Only the devices entered here are displayed on the SMIT menus when the user selects a backup.

-i "directory"

Specifies one or more directories, separated by spaces, to which the user can perform *network installation image* backups. This field applies only to the root user, because only the root user can create network installation image backups of volume groups. This flag applies only when you configure the root user or *all* users, if *root* is not specifically defined.

When backing up a volume group to use as a network installation image, the user has a disk image file backup option for each directory specified. Also, when this or other systems attempt to perform a network installation, all backup images in the specified directories that the client system has permission to read will be displayed as installation options.

-r Removes the specified user access record.

-u "user"

Specifies the user to be added, changed, or deleted.

Examples

1. To add user *peter* to the access list, providing access to local tape device */dev/rmt0*, virtual device *vdev0*, and the backup directory */usr/lpp/sysback/bf/local/peter*, type:

```
cfglocaccess -u peter -d "/dev/rmt0 vdev0" -b \  
/usr/lpp/sysback/bf/local/peter
```
2. To allow *all* users, except users *marsha* and *jan*, access to *all* devices, type:

```
cfglocaccess -u all -d "marsha jan" -f all
```
3. To remove the access record for user *cindy* from the access list, type:

```
cfglocaccess -r -u cindy
```
4. To list current hosts allowed to access local backup device access, list:

```
cfglocaccess -l
```

Files

/usr/lpp/sysback/.local_access List of local users allowed or denied access to the backup devices and directories for all SysBack backups. The format of the data in this file is very specific and should not be edited manually.

Related Information

The **cfgremserver** command.

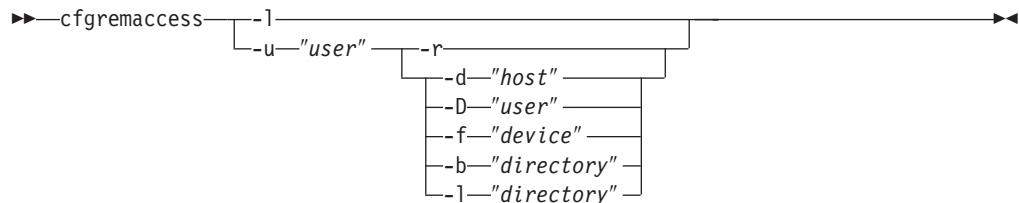
"Adding or Changing Local User Device/Directory Access" on page 7-2.

cfgremaccess

Purpose

Adds, lists, or removes remote host and user access to local backup devices and directories.

Syntax



Description

Before any client host can perform a backup to a remote server, the server must enable permission to the client host and to the specific users on the client who will be performing the backup operations. The **cfgremaccess** command provides access to the specified hosts and users. To provide the remote host a list of valid devices and backup files on this server when executing backups from SMIT, you must also run the **cfgremserver** command on the client to identify this server.

Before using this command, you must have already configured this host for Remote Services using the **cfgremsvs** command. You must also run the **cfgremsvs** command on the client host before attempting to execute any backups to this server.

You can provide all hosts on the network access to the server by creating a single record that applies to all of the hosts by providing a permission record for a host called *all*. You can exclude or deny specific hosts by using the **-d** flag. You can also create an access record for specific hosts, to override the *all* record for that host only.

Likewise, if you want to deny access to most, but not all, users on a particular host, you can indicate a user name of *all*. You can then supply a list of specific users to deny with the **-D** flag. You can also create a permission record for a specific host and user, to override any records for *all* hosts or *all* users.

Refer to “Adding or Changing the List of Remote Backup Servers” on page 8-8 for a complete explanation of the permissions and example of their use.

Note: You can enter either the hostname or a full domain name, if any. If you are operating in a domain network, use the full domain name of the client host. Using only the host name in a domain network allows access to any host on the network with the given host name, even though they might be in different domains.

Flags

-b “directory”

Specifies one or more directories to which the client hostname and username can perform regular image file backups. The client can perform a backup to

this directory or any of its subdirectories. A backup image file option for each directory supplied is displayed in SMIT when the user attempts to perform any backup, list, verify or restore operation.

-d "host"

Denies access to one or more specified hostnames. This flag is valid only when *all* is entered for the hostname (-h) parameter.

-f "device"

Specifies one or more devices to which the client hostname and username can perform regular image file backups. The entry can be a tape device (such as /dev/rmt0), virtual device (such as vdev0) or *all*, which allows the client to back up to any devices on this server. A device option for each device supplied is displayed in SMIT when the user attempts to perform any backup, list, verify, or restore operation. Also, these devices are listed when the client attempts to perform a network installation from this server.

-h "hostname"

Specifies the hostname of the client to add or remove. A hostname of *all* allows access to all hosts on the network. With a hostname of *all*, you can also enter hosts to exclude with the -d flag.

-i "directory"

Specifies one or more directories to which the client hostname and username can perform network installation image file backups. The client can perform a backup to this directory or any of its sub-directories. Any files in the directories supplied will be listed for the client when it attempts to perform a network installation operation.

- l Lists all hosts currently configured, along with the devices and directories to which they have access. When this flag is specified, any other flags used will be ignored.

-u "username"

Specifies the username on the client to add or remove. To allow access to all users on the specified hostname, enter the username *all*.

- r Removes the access record for the specified hostname and username. Removing the access record does not necessarily deny access to the client, because it might revert to access provided by another record.

-D "user"

Denies access to one or more specified user names. This flag is valid only when *all* is entered for the username (-u) parameter.

Examples

1. To add user *peter* on client host *pluto* to the access list, providing access to local tape device /dev/rmt0, virtual device *vdev0*, and the backup directory /usr/lpp/sysback/bf/pluto/peter, type:

```
cfgremaccess -h pluto -u peter -d "/dev/rmt0 vdev0" -b \  
/usr/lpp/sysback/bf/pluto/peter
```
2. To allow *all* users on *all* hosts, except users *marsha* and *jan* on host *mars*, access to all devices, type:

```
cfgremaccess -h all -d mars -u all -D "marsha jan" -f all
```
3. To remove the access record for user *cindy* on host *venus* from the access list, type:

```
cfgremaccess -r -h venus -u cindy
```
4. To list current hosts allowed local backup device access, type:

cfgremaccess -l

Files

/usr/lpp/sysback/.remote_access

List of hosts and users allowed or denied access to the local backup devices and directories for all SysBack backups. The format of the data in this file is very specific and should not be edited manually.

Related Information

The **cfgremsvs** and **cfgremserver** commands.

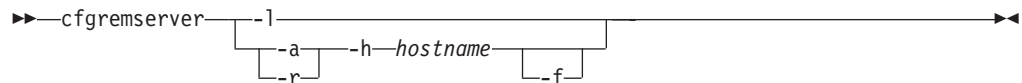
“Adding or Changing the List of Remote Backup Servers” on page 8-8.

cfgremserver

Purpose

Defines, lists, or undefines servers the client can access.

Syntax



Description

The **cfgremserver** command is used to either define or undefine a remote host that is to act as a server for the local host. The local system can execute remote sysback commands without setting up the server with this command, but only devices on remote servers set up with this command will be listed when executing backup, list, verify or restore options from SMIT. This command can also be used to list currently defined remote servers.

Before this command can be used to define a server to the system, both the local host and the host to act as the backup server must be configured for Remote Services using the **cfgremsvs** command. In addition, before a client machine can add a remote server, that server must have already provided access to its devices or directories with the **cfgremaccess** command. When defining a new remote server, this command verifies that Remote Services is configured on both the client and server systems and the server has granted access to this client.

Flags

- a Adds the hostname to the list of remote servers.
- f Indicates whether or not remote disk image file backup options should be displayed from SMIT. Without this option, disk image file options are not listed as valid backup devices even if the server has enabled directory access to this client.
- h **"hostname"**
Hostname of host where the requested backup device is attached.
- l Lists defined servers. Searches each server in the list to obtain a list of all devices and directories accessible by this client.
- r Removes the hostname from the list of remote servers.

Examples

1. To add server *venus* to the list and provide backup options on *venus* for devices or disk image files, type:
`cfgremserver -a -h venus -f`
2. To remove the server *venus* from the list of remote servers, type:
`cfgremserver -r -h venus`
3. To list currently defined servers and the devices available on those servers, type:
`cfgremserver -l`

Files

`/usr/lpp/sysback/.servers`

List of servers for which to list SMIT backup options

Related Information

The `cfgremsvs` and `chremaccess` commands.

cfgremsvs

Purpose

Configures Remote Services.

Syntax

►—cfgremsvs—◄

Description

This command is used to configure **Remote Backup Services** for either a host that is to act as a backup server for other machines or on a client that requires access to backup devices located on another backup server.

The command requires no arguments, and when executed, creates a new user ID “sbnet” in the *staff* group. This user ID is used to execute commands and transfer backup data using the **sbclient** command from the client to the server machine.

You need to run this command only once on each workstation.

Files

<code>/etc/password</code>	User password file
<code>/etc/group</code>	User group file
<code>/usr/lpp/sysback/.remote_access</code>	Access permissions for remote hosts

Related Information

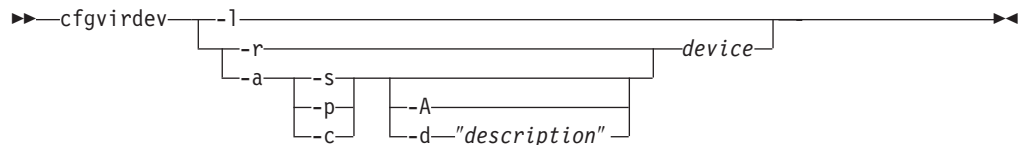
The **sbclient** command.

cfgvirdev

Purpose

Adds, lists, or removes virtual device descriptions.

Syntax



Description

The **cfgvirdev** command is used to add, list, or remove a virtual device description from the system. A virtual device can have a write policy of either **sequential**, **parallel** or **multi-copy**. Refer to Chapter 21, “Virtual Devices”, on page 21-1 for a detailed description of each write policy.

You can also indicate that a sequential **autoloader** is attached to the virtual device. This indicates that when a tape reaches the end of media, it is ejected from the drive, and the reading or writing continues automatically as soon as the next volume is inserted. In this case, the user receives no prompt to change the volume.

If you are creating an autoloader virtual device, you can assign one or more physical devices. Otherwise, you must assign multiple physical devices. A device is a tape drive such as `"/dev/rmt0"`.

You can assign your own description to the virtual device, or you can allow the system to provide a default description. By default, the description assigned will be either “Sequential Virtual Device”, “Parallel Virtual Device” or “Multi-copy Virtual Device”, depending on the write policy you choose.

When adding a new virtual device, the *device* option can be a single tape drive (such as `"/dev/rmt0"`) or a list of tape drives (such as `"/dev/rmt0 /dev/rmt1 /dev/rmt2"`). When removing a virtual device, the device option is the virtual device name to remove. Omit the *device* option when only listing defined virtual devices.

When adding a new virtual device, the system automatically assigns the next available virtual device name. The prefix will be *vdev*, followed by a device number, starting with 0 and increasing for each subsequent device added.

Flags

- a Adds a new virtual device.
- r Removes an existing virtual device.
- l Lists defined virtual devices.
- s When adding a virtual device, indicates a Sequential write-policy.
- p When adding a virtual device, indicates a Parallel write-policy.

- c When adding a virtual device, indicates a Multi-copy write-policy.
- d **"description"**
The description of the virtual device. This description is displayed on the SMIT screens when listing available backup and restore devices. Enclose this description in double quotation marks.
- A
Indicates an autoloader is attached to the physical devices.

Examples

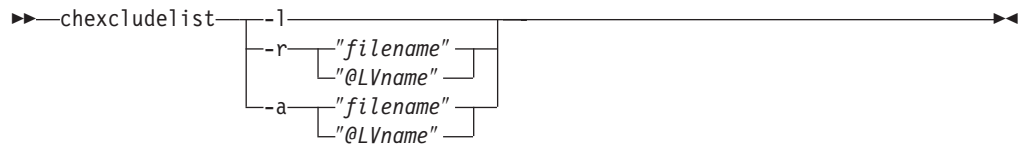
1. To create a sequential virtual device, using tape devices *rmt0* and *rmt1*, type:
`cfgvirdev -as /dev/rmt0 /dev/rmt1`
2. To create a parallel virtual device using devices *rmt1* and *rmt2*, and assigning a user description, type:
`cfgvirdev -apd "Parallel 8mm tapes" /dev/rmt1 /dev/rmt2`
3. To define *rmt0* as an auto-loader, type:
`cfgvirdev -asd "Autoloader" /dev/rmt0`
4. To remove virtual device *vdev0*, type:
`cfgvirdev -r vdev0`

chexcludelist

Purpose

Adds, removes, or lists files or directories in the exclude list file.

Syntax



Description

The **chexcludelist** command is used to either add or delete entries from the exclude list file. The exclude list file contains directories, individual filenames, or logical volume names that are to be excluded from all backups created with the SysBack commands.

The file or directory name must begin with a slash (/) but can contain *wildcard* (*) characters. If you enter a filename, only that file is excluded. If you enter a directory name, all files and directories within the specified directory are excluded. When specifying wild cards, you must enclose the string in single quotation marks (') to preserve the special characters.

The following are examples of using wildcard in the exclude list:

/tmp	All files below the /tmp directory
/*test*	All files in the system containing the word "test".
/*old	All files on the system ending with "old".
/home/b*	All files under /home starting with a "b".
/home/t*y	All files under /home starting with "t" and ending with "y".

Note that any entry starting with "/" will include all directories on the system, not just the root (/) directory.

Note: When excluding a logical volume name, type a "@" character before the logical volume name. This indicates that the entry is a logical volume and not a file or directory. You cannot use wild cards in logical volume names.

Flags

- l** Lists current entries. No changes are made to the existing exclude list.
- a "filename"**
Adds a filename or directory to the exclude list.
- r "filename"**
Removes a filename or directory from the exclude list.

Examples

1. To add the directory **/tmp** to the exclude list, type:
`chexcludelist -a /tmp`
2. To exclude all files on the system ending with “.old”, type:
`chexcludelist -a ©/*.*old©`
3. To exclude logical volume *userlv1* from volume group backups, type:
`chexcludelist -a @userlv1`
4. To remove the file **/home/test** from the exclude list, type:
`chexcludelist -r /home/test`
5. To list current excluded files and directories, type:
`chexcludelist -l`

Files

/usr/lpp/sysback/.exclude_list Filenames and directories to exclude from backups.

editlvminfo

Purpose

Customizes an LVM information file.

Syntax

```
►►—editlvminfo—f—"filename"——————◄◄
```

Description

The **editlvminfo** command reads the contents of the *LVM information file*, specified by the *filename* parameter and initializes the user interface used for changing the volume group, logical volume, and filesystem information within the file.

This option is usually used to customize a file, created with the **mkvginfo** command, before including the customized file on a backup, using the **-g** flag with either the **mklvback**, **mkjfsback**, **mkvgback** or **sysback** commands.

The user interface provides options for changing any of the information in the file, such as assigning new physical volumes to volume groups, changing the volume group where a logical volume or filesystem exists, and changing the sizes of logical volumes and filesystems.

Detailed instructions for changing the information in the LVM information file is in Chapter 11, "Changing the Volume Group, Logical Volume and Filesystem Attributes", on page 11-1.

Related Information

The **mkvginfo**, **mklvback**, **mkjfsback**, **mkvgback** or **sysback** commands.

Chapter 11, "Changing the Volume Group, Logical Volume and Filesystem Attributes", on page 11-1.

getlvminfo

Purpose

Displays Logical Volume Manager (LVM) information for volume groups, logical volumes, and physical volumes.

Syntax

```
➤➤getlvminfo -V Option -l Option -P Option -G Option➤➤
```

-V Option:

```
|--V "VGname" --c --d --i --l --q --x --A --S --1 --p I --p N --p X|
```

-l Option:

```
|--l "LVname" --a --b --c --d --e --i --l --w --x --z --X --Z --1 --p --m --I --N --X --h|
```

-P Option:

```
|--P "PVname" --a --l --n --v --x --A --S --1 --I --N --X|
```

-G Option:

```
|--G "PVname" --c --d --i --l --s --X --1 --p I --p N --p X --I --N|
```

Description

This command is used to display all available *Logical Volume Manager* information for volume groups, physical volumes, and logical volumes. It retrieves LVM information for all SysBack commands requiring LVM data. The **getlvminfo** command is faster and easier than using the standard AIX LVM commands and provides the information in a simple, reliable format.

At least one argument is required. If only a single argument (**-V** or **-P**) is specified, all volume groups or physical volumes on the system, respectively, are displayed.

Any time the **-I**, **-N** or **-X** arguments are used, any physical volumes are displayed using the *PVID*, *PV Name* or *PV Location*, respectively.

One of the flags **-V**, **-P**, **-L** or **-G** must be specified to display attributes for a volume group, physical volume, or logical volume. The **-G** flag can also display volume group information for a volume group that is not currently varied on.

Flags

- 1** Displays all output on a single line, separated by spaces. The default is to show each attribute on a separate line.
- a** When used with the **-L** flag, displays the intra-physical volume policy for a logical volume. When used with the **-P** flag, displays currently allocated physical partitions for a physical volume.
- b** Used with the **-L** flag to display whether or not bad block relocation is enabled for a logical volume.
- c** When used with **-V** or **-G** flag, indicates whether or not a volume group is concurrent-capable. When used with **-L** flag, indicates the number of copies for a logical volume.
- d** With the **-V** or **-G** flag, indicates the number of physical volumes assigned to the volume group. When the **-L** flag, indicates a mirror scheduling policy of either parallel (p) or sequential.
- e** Used with the **-L** flag, displays the intra-physical volume policy for a logical volume.
- h** Displays a more detailed usage message for the **getlvminfo** command to standard error.
- i** With the **-V** or **-G** flag, displays the *volume group ID* (VGID); with the **-L** flag, displays the *logical volume ID* (LVID); and with the **-P** flag, displays the *physical volume ID* (PVID).
- l** Used with the **-V** or **-G** flag to list all logical volumes names in the volume group. With the **-L** flag, indicates the logical volume *label*.
- m** Used with **-L** flag to list a *physical partition map* for the logical volume. This flag cannot be used with the **-p** flag.

- n** With the **-L** flag, indicates the number of *logical partitions* (LPs) assigned to the logical volume. With the **-P** flag, displays the total *physical partitions* (PPs) available on the physical volume.
- p** With the **-V** or **-G** flag, displays the physical volumes in the volume group. With the **-L** flag, displays the physical volumes on which a logical volume resides. This flag cannot be used with the **-m** flag.
- q** Used with the **-V** flag to indicate whether or not *quorum checking* is enabled for a volume group.
- r** Used with the **-L** flag to indicate whether or not the logical volume is *relocatable*.
- s** Used with the **-L** flag to indicate whether or not a *strict allocation policy* is enabled for a logical volume, preventing a single copy from being placed on multiple physical volumes.
- t** Used with the **-L** flag to display the logical volume type.
- u** Used with the **-L** flag to display the *upperbound limit* (maximum PVs) for the logical volume.
- v** With **-L** flag, displays whether or not *write-verification* is enabled. With the **-P** flag, displays the number of *volume group descriptor areas* (VGDAAs) on the physical volume.
- w** With **-L** flag, displays whether or not *mirror-write-consistency checking* (MWC) is enabled.
- x** With the **-V** flag, indicates whether or not the volume group is varied on in *concurrent mode*. With the **-L** flag, indicates the *maximum logical partitions* (LPs) for the logical volume.
- z** With the **-L** flag, indicates the logical volume *stripe size*. A value of zero (0) indicates that striping is disabled.
- A** With the **-V** flag, indicates whether or not the volume group is automatically varied on at system startup.
- G "PVname"** Displays volume group information using the physical volume name instead of the volume group name.
- I** Whenever physical volume information is displayed, this flag indicates that the physical volumes should be displayed using the *physical volume ID* (PVID). This is the default.
- L "LVname"** Displays attributes for the logical volume name specified.
- N** Whenever physical volume information is displayed, this flag displays physical

volumes using the physical volume name (hdiskX) rather than the PVID. When displaying a list of volume groups using the **-V** flag, this flag displays the volume groups by name rather than VGID.

-P "PVname"

When used without specifying a physical volume name, this flag displays a list of physical volumes on the system. When a physical volume name is specified, this flag displays the attributes for the specified physical volume.

-S With **-V** or **-G** flag, displays the *physical partition size* in megabytes. With the **-L** flag, displays the *logical volume state* as either syncd (0) or stale (1). With the **-P** flag, displays the *physical volume state* of either active (0), removed/missing (1), or stale (2).

-V "VGname"

When used without specifying a volume group name, this flag displays a list of volume groups on the system. Use with the **-N** flag to display the volume group list by volume group name instead of VGID. When a volume group name is provided, this flag displays the attributes for the specified volume group.

-X Any time physical volumes are displayed with this command, displays them by location code rather than by PVID.

-Z

Used with the **-L** flag to indicate the *stripe width* (number of physical volumes used in striping) for the logical volume. If a value of zero (0) is returned, striping is disabled.

Examples

1. To list the logical volumes in the *rootvg* volume group:
`getlvminfo -V rootvg -l`
2. To list the *Intra-PV policy*, *Inter-PV policy*, number of copies and number of *logical partitions* for the *userlv1* logical volume on a single line:
`getlvminfo -L userlv1 -aecn1`
3. To list the physical volumes in the *uservg* volume group by location code:
`getlvminfo -V uservg -pX`
4. To show the physical partition map for the *data1v2* logical volume in the form "*hdiskname:PPnumber*":
`getlvminfo -L data1v2 -mN`

lscfginfo

Purpose

Prints or displays a report of the Logical Volume Manager configuration.

Syntax

```
➤—lscfginfo—f—"filename"—➤
               |
               |—q—"queue"—➤
```

Description

This command prints, displays, or saves to file a report containing the system configuration. This includes all information pertaining to the volume groups, physical volumes, logical volumes, and filesystems. This report contains all of the key information that might be necessary for rebuilding various components of the system in case of system failures.

In most cases, it is not necessary to use this information to recover from system failures, because the SysBack installation process and the **remakevg** command recreate volume groups, logical volumes, and filesystems without requiring the user to have knowledge of the system configuration. This information, however, can be useful in planning a migration of filesystems to new hardware or in reorganizing an existing system to take advantage of disk striping, mirroring, and other features.

The report output includes the following information:

Volume group information:

One record for each volume group. Contains all volume group attributes and physical volume sizes. Example:

Volume Group	Auto-on?	PP Size	Quorum?	Total	Used	Free	PV(s)
rootvg	y	4 MB	y	250 PPs 1002 MB	213 PPs 852 MB	37 PPs 148 MB	hdisk0

Logical Volume Information:

One record for each logical volume. Contains most logical volume attributes and a list of the physical volumes where each logical volume resides. Example:

Volume Group	Logical Volume	Attributes			
rootvg	hd8	Type:	jfslog	Copies:	1
		LPs:	1	IntraPV:	c
		MinLps:	0	InterPV:	m
		PV(s):	hdisk0	Upper:	32
				StrpSz:	0

Physical Volume Information:

One record for each physical volume. Contains the physical volume location, size, and a map of the regions on the disk where each logical volume resides. Example:

PV Name	Volume Group	Location	PVID	MB	PPs
hdisk0	rootvg	00-00-0S-0,0	00000218acd0f607	1002	250
	LV Name	PPs	Region		
	hd8	101X.....		
	hd6	51-62	..X.....		

	73-96	..XX.....
hd4	3	X.....
	102-103X.....
hd3	105-109X.....
hd2	5-27	XX.....
	110-207XXXXX.
	222-242X

Filesystem information:

Contains all filesystem attributes. Note that the “BF Spt” and “AG” Size fields are displayed only on AIX 4.2 or later systems.

Example:

Volume Group	Mount Point	FragSz	NBPI	Cmprs	BF Spt?	AG Size?
rootvg	/	4096	2048	no	n	8
	/home	512	4096	no	y	8
	/tmp	4096	4096	no	n	8
	/usr	4096	4096	no	n	8
	/var	512	4096	no	n	8
	/data/files	512	4096	no	y	32

Logical Volume Partition Maps:

Shows the specific physical partitions on the physical volumes that are used by each logical volume. This is helpful in determining the fragmentation of logical volumes.

Example:

Volume Group	Logical Volume	Copy#	PV Name	PP#s	PV Region
rootvg	hd8	1	hdisk0	101-101X.....
	hd6	1	hdisk0	51-62	..X.....
		1	hdisk0	73-96	..XX.....
	hd4	1	hdisk0	3	X.....
		1	hdisk0	102-103X.....
	hd3	1	hdisk0	105-109X.....
	hd2	1	hdisk0	5-27	XX.....
		1	hdisk0	110-207XXXXX.
		1	hdisk0	222-242X

Flags

-f “filename”

Saves the report in the named file. When used, no information is displayed on the screen.

-p “queue”

Sends the report to the named print queue. When used, no information is displayed on the screen.

Related Information

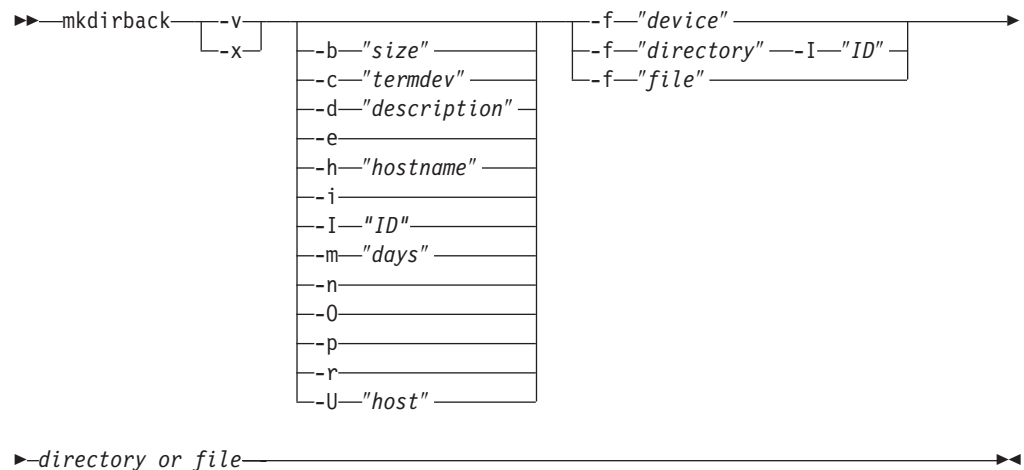
The **getlvminfo** command.

mkdirback

Purpose

Backs up specified files or directories.

Syntax



Description

The **mkdirback** command is used to back up specific files or directories. You must choose a starting directory to back up that directory and any sub-directories.

You can specify a single directory or multiple directories to include all of those directories in a single backup. You can also specify specific filenames to back up only those files. Filenames must be specified relative to the root directory by preceding the filename with a slash (/).

The backup can be performed to a tape drive, virtual device, or disk image file. When specifying a disk image file, you can enter the full pathname of the file to create or overwrite. When doing so, the filename must begin with the prefix "FD". to indicate the file is a file/directory backup. You can also specify only the backup directory and a *unique ID*. When doing so, a filename is created for you. Refer to "Backups to Disk Image Files" on page 2-6 for information on the filename created. If you are creating a file and a file by the same name already exists, specify the **-O** option to overwrite the existing file.

The backup can also be performed to a remote device, virtual device, or disk image file. If *Remote Services* has been configured on both the local and server system using the **cfgremsvs** command, and you have defined a backup device on the server for this system using the **cfgremaccess** command, then you can also select a *hostname* using the **-h** option. The backup will then be written to the *device* or *filename* on the specified server, provided the server has enabled this system access to the specified device or directory.

Files, or files within directories, that are specified in the exclude list are not backed up with this command. See **chexcludelist** command for information on creating exclude lists.

Unlike all other backup types, this type of backup contains no *Logical Volume Manager* (LVM) information. Therefore, it is not possible to use this backup, regardless of its contents, for recreating volume groups, logical volumes, and filesystems. Using this backup option for backing up all files on the system (from the / directory) cannot provide a backup that can be used to reinstall the system.

Some files and directories on the system, such as certain contents of the root (/) and /usr filesystems, should never be restored from a backup, as this would adversely affect the active system configuration and can cause either system errors or a complete system failure. Use this command only to back up files and directories that contain non-system-related information, such as user data, application programs, and so on.

Using the **-m** option, you can also specify to back up only files that have been modified within a certain number of days. This is useful for performing daily backups. Be aware, however, that a day is considered exactly 24 hours. Therefore, always back up at least every 24 hours when specifying the **-m1** option. If, for instance, your backups were performed 1/2 hour later today than yesterday, neither today's nor yesterday's backup will contain any files changed within that 1/2 hour. It is a good idea to use **-m2** each day to ensure that no files will be skipped regardless of the time the backup is performed.

Always perform a backup of all files, regardless of date, before performing partial backups using the **-m** option. If you later need to restore files or directories, restore them from a full backup, and then restore each partial backup created after the full backup.

The backup can also be performed as a "pull" backup to enable central management of backups. The machine that "pulls" the backup is called the "initiator," while the machine that is backed up is called the "backup system." The machine that receives the backup data is called the "destination system."

The initiator is the machine where the `mkdirback` command is issued. The backup system is referenced in the command syntax by the **-U "host"** flag. The data destination system is referenced by the **-h "host flag"**.

When only the **-U "host"** flag is specified, the **-f "device"** flag refers to a device on the initiator system. In this case, the backup destination and the initiator are the same system. This is known as a "two-way pull backup."

When the **-U "host"** and **-h "host"** flags are specified, the **-f "device"** flag refers to a device on the host specified by the **-h "host"** flag. In this case, the backup destination and the initiator are different systems. This is known as a "three-way pull backup."

Remote Services must be configured, using the `cfgremsvs` command, on all of the machines involved in the backup operation, the initiator, the backup system, and the data destination machines. The backup destination machine must have the Server Options of Remote Services configured to allow the backup system machine to send its data to devices on the backup destination machine. You can do this with the **Add or Change Client Host Access to this Server** option or the `cfgremaccess` command.

The backup system machine must have the Client Options of Remote Services configured to specify the backup destination machine as a backup host. You can do this with the **Add or Change List of Remote Backup Servers** option or the **cfgremserver** command.

The backup system must also configure Remote Command Access to allow the initiator machine to pull the backup.

Flags

-b "size"

Specifies the buffer size in K-bytes (1024-bytes). Changing this value either increases or decreases the amount of data written to the output device at one time. Some devices with small buffers might require you to reduce this value, while other devices with very large buffers can benefit from increased performance by increasing this value. If you are unsure, use the default value (64 Kbytes).

-c "termdev"

If the backup spans multiple tape volumes, the volume prompt is sent to the *termdev* device (such as */dev/tty0*). If the **-h hostname** option is specified, this flag specifies the device on the remote host.

-d "description"

A custom description to be included in the backup header. If the description includes spaces, the entire description must be enclosed in double quotation marks ("").

-e Forwards to the end of the last SysBack backup on the tape and is used when stacking multiple backups on one tape.

-f "device, file or directory"

Specifies the output device name, filename, or directory for the backup. The specified output option can be on the local system or server (if **-h** option provided). Device name can be a tape drive or virtual device name. If you specify a directory, you must also specify an *ID* using the **-I** flag.

-h "hostname"

Name of the host to receive the backup data (for example, the data destination host). This is the host that provides the backup device specified using the **-f** flag.

-I "ID"

This option is used only if a directory is specified as the output device. The ID is included in the filename created to make it unique from other disk image file backups. If a backup in the same directory with this ID already exists, specify the **-O** flag to overwrite the previous backup.

-m "days"

Specifies that only files modified within a given number of days will be backed up.

-n

Indicates that the tape should not be rewound at the beginning of the backup. Using this flag enables this backup to be appended to the previous backup performed. The tape is not automatically rewound at the end of the backup. The **-n** option is always ignored when backing up to a non-tape device.

-p

Indicates that the data should be packed before being written to the media.

This typically reduces size of backup between 25% and 40%. For increased performance, do not use this options when backing up to a device that provides hardware data compression.

-O

If a filename was specified as the output device and the filename already exists, overwrites the previous file with the new backup.

-r user=[u | a]

Specifies user read permission when backing up to a disk image file. “**u**” indicates only the specified user can read the file. “**a**” indicates that any user can read the file.

-r host=[h | a]

Specifies host read permission when backing up to a disk image file. “**h**” indicates only this host can read the file. “**a**” indicates any host can read the file.

-U “host”

The name of the host to be backed up (such as the backup system).

-v Specifies that file names should be listed on the screen as the files are being backed up. This flag cannot be used with the **-x** flag.

-x Specifies that the progress indicator should be shown on the screen, displaying the approximate size and time to read the entire contents of the media and the amount completed. This flag cannot be used with the **-v** flag.

Examples

1. To perform a backup of the **/home/tony** directory to the backup directory **/usr/lpp/sysback/bf/root**, allowing only this user and host to read the file, and to display a progress indicator, type:

```
mkdirback -f /usr/lpp/sysback/bf/root -x -r host=h -r user=u -I  
tony_tuesday /home/tony
```

The above will create a file called
/usr/lpp/sysback/bf/root/FD.hostname.tony_tuesday.

2. To perform a remote push backup to virtual device *vdev2* on host *jupiter* and to make this a compressed backup of the **/data/file1** and **/data/file2** files, type:

```
mkdirback -Dph jupiter -f vdev2 /data/file1 /data/file2
```

3. To perform a backup to *rmt1* on the local system of only the files in the **/usr** and **/var** directories that have changed within the last seven days, type:

```
mkdirback -nm7 -f /dev/rmt1 /usr /var
```

4. To initiate a pull backup of **/home** on host *lasher*, from host *sysback1*, and send the data to *rmt1* of the host *sysback1*, type the following from *sysback1*:

```
mkdirback -U lasher -f /dev/rmt1 /home
```

5. To initiate a pull backup of **/home** on host *lasher*, from host *sysback1*, and send the data to *rmt1* of the host *shappy*, type the following from *sysback1*:

```
mkdirback -U lasher -h shappy -f /dev/rmt1 /home
```

Related Information

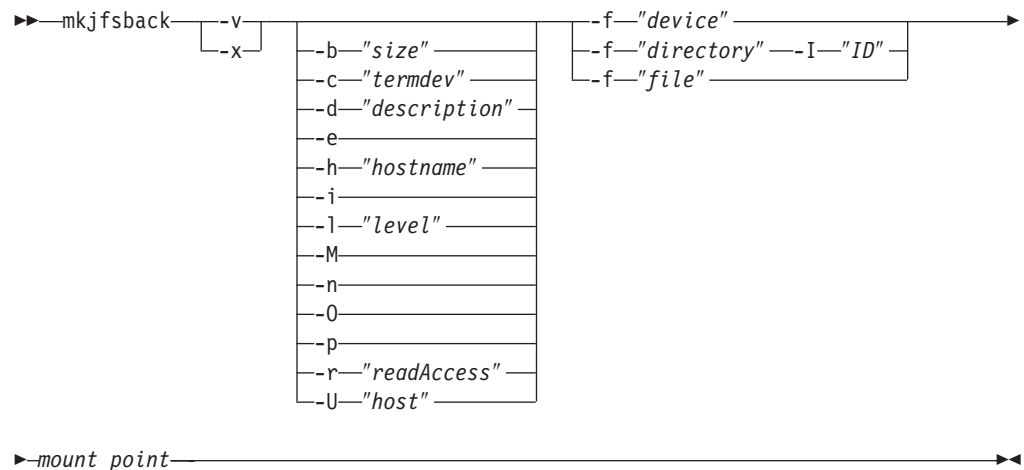
The **sysrestore**, **cfgremsvs**, **cfgremaccess**, **chexcludelist**, and **cfgremrootaccess** commands.

mkjfsback

Purpose

Performs a backup of one or more filesystems.

Syntax



Description

The **mkjfsback** command is used to perform a backup of one or more filesystems. The mount point parameter, which is the directory name where each filesystem is mounted (such as **/home**), indicates the filesystems to include. You can back up multiple filesystems by appending each mount point to the end of the command, separated by spaces.

The backup can be performed to a tape drive, virtual device, or disk image file. When specifying a disk image file, you can enter the full pathname of the file to create or overwrite. When doing so, the filename must begin with the prefix "FS" to indicate the file is a filesystem backup. You can also specify only the backup directory and a unique ID. When doing so, a filename will be created for you. Refer to "Backups to Disk Image Files" on page 2-6 for information on the filename created. If you are creating a file and a file by the same name already exists, specify the **-O** option to overwrite the existing file.

The backup can also be performed to a remote device, virtual device, or disk image file. If *Remote Services* has been configured on both the local and server system using the **cfgremsvs** command, and you have defined a backup device on the server for use by this system using the **cfgremaccess** command, then you can also select a *hostname* using the **-h** option. The backup will then be written to the device or *filename* on the specified server, provided the server has enabled this system access to the specified device or directory.

A level 0 backup must be performed before any level 1-9 can be performed. Refer to "Understanding Incremental Backups" on page 4-1 for additional details on incremental backups.

This command does not back up files, or files within directories, that are specified in the exclude list. See the **chexcludelist** command for information on creating exclude lists.

The backup can also be performed as a “pull” backup to enable central management of backups. The machine that “pulls” the backup is called the “initiator,” while the machine that is backed up is called the “backup system.” The machine that receives the backup data is called the “destination system.”

The initiator is the machine where the **mkdirback** command is issued. The backup system is referenced in the command syntax by the **-U “host”** flag. The data destination system is referenced by the **-h “host flag”**.

When only the **-U “host”** flag is specified, the **-f “device”** flag refers to a device on the initiator system. In this case, the backup destination and the initiator are the same system. This is known as a “two-way pull backup.”

When the **-U “host”** and **-h “host”** flags are specified, the **-f “device”** flag refers to a device on the host specified by the **-h “host”** flag. In this case, the backup destination and the initiator are different systems. This is known as a “three-way pull backup.”

Remote Services must be configured, using the **cfgremsvs** command, on all of the machines involved in the backup operation, the initiator, the backup system, and the data destination machines. The backup destination machine must have the Server Options of Remote Services configured to allow the backup system machine to send its data to devices on the backup destination machine. You can do this with the **Add or Change Client Host Access to this Server** option or the **cfgremaccess** command.

The backup system machine must have the Client Options of Remote Services configured to specify the backup destination machine as a backup host. You can do this with the **Add or Change List of Remote Backup Servers** option or the **cfgremserver** command.

The backup system must also configure Remote Command Access to allow the initiator machine to pull the backup.

Flags

-b “size”

Specifies the buffer size in K-bytes (1024-bytes). This value either increases or decreases the amount of data that is written to the output device at one time. Some devices with small buffers might require you to reduce this value, while other devices with very large buffers can benefit from increased performance by increasing this value. If you are unsure, use the default value (64 Kbytes).

-c “termdev”

If the backup spans multiple tape volumes, the volume prompt is sent to the *termdev* device (such as */dev/tty0*). If the **-h hostname** option is specified, this flag specifies the device on the remote host.

-d “description”

A custom description to be included in the backup header. If the description includes spaces, the entire description must be enclosed in double quotation marks (“”).

- e Forwards the tape to the end of the last Sysback backup. Used when stacking multiple backup images on a tape.
- f **"device, file or directory"**
Specifies the output device name, filename, or directory for the backup. The specified output option can be on the local system or server (if **-h** option provided). The device name can be a tape drive or virtual device name. If you specify a directory, you must also specify an *ID* using the **-I** flag.
- g **"filename"**
Indicates the name of an *LVM Information File* previously created and customized for this backup. Refer to the **mkvginfo** and **editlvminfo** commands.
- h **"hostname"**
Name of the remote backup server host to receive the backup data (such as the data destination host). This is the host that provides the backup device specified by the **-f** flag.
- i Indicates to dynamically create a backup file ID when writing backups to disk image file. This flag supersedes the **-I"ID"** flag.
- I **"ID"**
This option is used only if a directory is specified as the output device. The ID is included in the filename created to make it unique from other disk image file backups. If a backup in the same directory with this ID already exists, specify the **-O** flag to overwrite the previous backup.
- l **"level"**
Specifies the backup level (default is 0, or all files). Valid values are 0-9. Only files created or changed since the last (*level* - 1) backup was performed.
- M
Retains physical partition mapping, by default, when the logical volume is recreated from this backup. Unless the logical volume was originally created using a physical partition map, it is generally recommended that it not be recreated using the same partitions, as this would preserve fragmentation that develops over time as logical volumes and filesystems are expanded. You can specify whether or not partition mapping will be used before recreating the logical volume.
- n
Indicates that the tape should not be rewound at the beginning of the backup. This enables the backup to be appended to the previous backup performed. The tape is not automatically rewound at the end of the backup. The **-n** option is always ignored when backing up to a non-tape device.
- O
Overwrites the previous file, if a filename was specified as the output device, and the filename already exists.
- P
Indicates that the data should be packed before being written to the media. This typically reduces size of backup between 25% and 40%. For increased performance, do not use this option when backing up to a device that provides hardware data compression.
- r **user=[u | a]**
Specifies user read permission when backing up to a disk image file. **"u"** indicates only the specified user can read the file. **"a"** indicates that any user can read the file.

-r host=[h | a]

Specifies host read permission when backing up to a disk image file. “h” indicates only the specified host can read the file. “a” indicates that any host can read the file.

-U “host”

Name of the host to be backed up (such as the backup system).

-v Specifies that file names should be listed on the screen as the files are being backed up. This flag cannot be used with the **-x** flag.

-x Specifies that the progress indicator should be shown on the screen, displaying the approximate size and time to read the entire contents of the media and the amount completed. This flag cannot be used with the **-v** flag.

Examples

1. To perform a local backup of the /home filesystem to the directory **/usr/lpp/sysback/bf/mars**, indicating that only this host and user can read the file and to display a progress indicator, type:

```
mkjfsback -f /usr/lpp/sysback/bf/mars -I home4me -x \  
-r host=h -r user=u /home
```

The filename created will be **/usr/lpp/sysback/bf/mars/FS.hostname.home4me**.

2. To perform a level 1 backup of the /data/files and /sales filesystems as a remote push backup to **/dev/rmt1** on the host *jupiter*, type:

```
mkjfsback -l1 -h jupiter -f rmt1 /data/files /sales
```

Note that a level 0 backup must have previously been created before a level 1 can be performed.

3. To perform a level 9 backup of the /home filesystem to the local virtual device *vdev1*, type:

```
mkjfsback -n19 -f vdev1 /home
```

Note that the **-n** option is specified. This prevents the tape drive from being rewound before the backup begins, enabling this backup to be “stacked” on the end of the previous backup image.

4. To initiate a pull backup of the /home filesystem on host *lasher*, from host *sysback1*, and send the data to *rmt1* of the host *sysback1*, type the following from *sysback1*:

```
mkjfsback -U lasher -f /dev/rmt1 /home
```

5. To initiate a pull backup of the /home filesystem on host *lasher*, from host *sysback1*, and send the data to *rmt1* of the host *shappy*, type the following command from *sysback1*:

```
mkjfsback -U lasher -h shappy -f /dev/rmt1 /home
```

Related Information

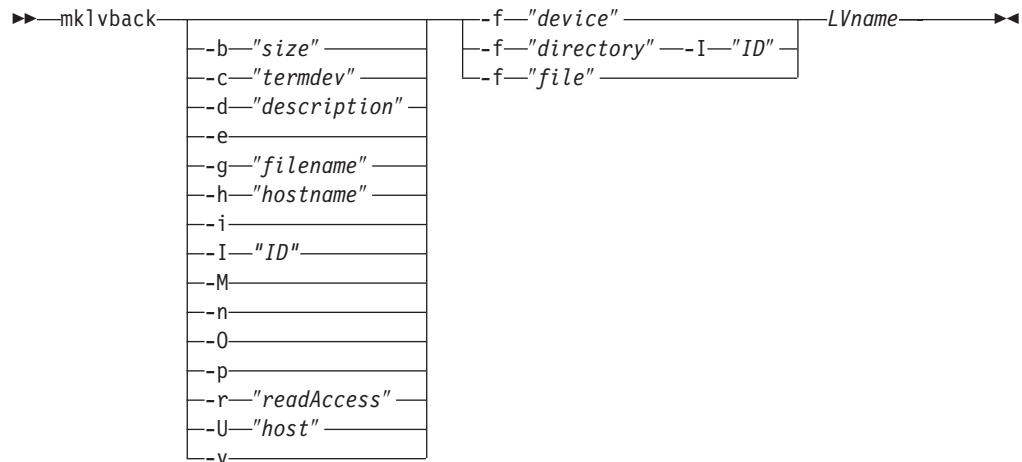
The **sysrestore**, **cfgremsvs**, **cfgremaccess**, **mkvginfo**, **editlvminfo**, **cfgremrootaccess**, and **chexcludelist** commands.

mklvback

Purpose

Performs a backup of logical volumes.

Syntax



Description

The **mklvback** command is used to back up data from one or more logical volumes. This option reads the entire logical volume, copying all “raw” data to the specified output device or file. Many database applications use a raw logical volume to store data, but AIX is unaware of the format of the data within the logical volume. Therefore, this option copies the entire contents of the logical volume, even though the application might have written to only a small portion of the total logical volume size.

The backup can be performed to a tape drive, virtual device, or disk image file. When specifying a disk image file, you can enter the full pathname of the file to create or overwrite. When doing so, the filename must begin with the prefix “LV” to indicate the file is a logical volume backup. You can also specify only the backup directory and a *unique ID*. When doing so, a filename will be created for you. Refer to “Backups to Disk Image Files” on page 2-6 for information on the filename created. If you are creating a file and a file by the same name already exists, specify the **-O** option to overwrite the existing file.

The backup can also be performed to a remote device, virtual device, or disk image file. If *Remote Services* has been configured on both the local and server system using the **cfgremsvs** command, and you have defined a backup device on the server for use by this system using the **cfgremaccess** command, then you can also select a hostname using the **-h** option. The backup will then be written to the device or filename on the specified server, provided the server has enabled this system access to the specified device or directory.

You must supply one or more logical volume names with this command. Do not include the “/dev/” prefix with the logical volume name. If specifying more than one logical volume, append each logical volume to the end of the command, separated by spaces.

The backup can also be performed as a “pull” backup to enable central management of backups. The machine that “pulls” the backup is called the “initiator,” while the machine that is backed up is called the “backup system.” The machine that receives the backup data is called the “destination system.”

The initiator is the machine where the `mkdirback` command is issued. The backup system is referenced in the command syntax by the **-U “host”** flag. The data destination system is referenced by the **-h “host flag”**.

When only the **-U “host”** flag is specified, the **-f “device”** flag refers to a device on the initiator system. In this case, the backup destination and the initiator are the same system. This is known as a “two-way pull backup.”

When the **-U “host”** and **-h “host”** flags are specified, the **-f “device”** flag refers to a device on the host specified by the **-h “host”** flag. In this case, the backup destination and the initiator are different systems. This is known as a “three-way pull backup.”

Remote Services must be configured, using the `cfgremsvs` command, on all of the machines involved in the backup operation, the initiator, the backup system, and the data destination machines. The backup destination machine must have the Server Options of Remote Services configured to allow the backup system machine to send its data to devices on the backup destination machine. You can do this with the **Add or Change Client Host Access to this Server** option or the `cfgremaccess` command.

The backup system machine must have the Client Options of Remote Services configured to specify the backup destination machine as a backup host. You can do this with the **Add or Change List of Remote Backup Servers** option or the `cfgremserver` command.

The backup system must also configure Remote Command Access to allow the initiator machine to pull the backup.

Flags

-b “size”

Specifies the buffer size in K-bytes (1024-bytes). This value either increases or decreases the amount of data that is written to the output device at one time. Some devices with small buffers might require you to reduce this value, while other devices with very large buffers can benefit from increased performance by increasing this value. If you are unsure, use the default value (64 Kbytes).

-c “termdev”

If the backup spans multiple tape volumes, the volume prompt is sent to the *termdev* device (such as `/dev/tty0`). If the **-h hostname** option is specified, this flag specifies the device on the remote host.

-d “description”

A custom description to be included in the backup header. If the description includes spaces, the entire description must be enclosed in double quotation marks (“”).

-e Forwards to the end of the last SysBack backup on the tape. Used when stacking multiple backups on one tape.

-f “device, file or directory”

Specifies the output device name, filename, or directory for the backup. The

specified output option can be on the local system or server (if **-h** option provided). The device name can be a tape drive or virtual device name. If you specify a directory, you must also specify an *ID* using the **-I** flag.

-g "filename"

Indicates the name of an *LVM Information File* previously created and customized for this backup. Refer to the **mkvginfo** and **editlvminfo** commands.

-h "hostname"

Name of the remote backup server host to receive the backup data (such as the data destination host). This is the host that provides the backup device specified by the **-f** flag.

-i Indicates to dynamically create a backup file ID when writing backups to disk image file. This flag supersedes the **-I"ID"** flag.

-I "ID"

This option is used only if a directory is specified as the output device. The ID is included in the filename created to make it unique from other disk image file backups. If a backup in the same directory with this ID already exists, specify the **-O** flag to overwrite the previous backup.

-l "level"

Specifies the backup level (default is 0, or all files). Valid values are 0-9. Only files created or changed since the last (level - 1) backup was performed.

-n

Indicates that the tape should not be rewound at the beginning of the backup. This enables the backup to be appended to the previous backup performed. The tape is not automatically rewound at the end of the backup. The **-n** option is always ignored when backing up to a non-tape device.

-O

Overwrites the previous file, if a filename was specified as the output device, and the filename already exists.

-P

Indicates that the data should be packed before being written to the media. This typically reduces size of backup between 25% and 40%. For increased performance, do not use this option when backing up to a device that provides hardware data compression.

-r user=[u | a]

Specifies user read permission when backing up to a disk image file. "**u**" indicates only the specified user can read the file. "**a**" indicates that any user can read the file.

-r host=[h | a]

Specifies host read permission when backing up to a disk image file. "**h**" indicates only the specified host can read the file. "**a**" indicates that any host can read the file.

-U "host"

Name of the host to be backed up (such as the backup system).

-x Specifies that the progress indicator should be shown on the screen, displaying the approximate size and time to read the entire contents of the media and the amount completed. This flag cannot be used with the **-v** flag.

-M

Retains physical partition mapping, by default, when the logical volume is

recreated from this backup. Unless the logical volume was originally created using a physical partition map, it is generally recommended that it not be recreated using the same partitions, as this would preserve fragmentation that develops over time as logical volumes and filesystems are expanded. You can specify whether or not partition mapping will be used before recreating the logical volume.

Examples

1. To perform a local backup of the `lv02` logical volume to the directory `/usr/lpp/sysback/bf/root`, indicating that only this user and host can read the file and displaying a progress indicator, type:

```
mklvback -f /usr/lpp/sysback/bf/root -I lv02 -x -r host=h -r user=u lv02
```

The filename created will be `/usr/lpp/sysback/bf/root/LV.hostname.lv02`.

2. To perform a remote push backup to the virtual device `vdev2` of the host *jupiter* and to make this a compressed backup of the logical volumes *data1v* and *data1v2*, type:

```
mklvback -nph jupiter -f vdev2 data1v data1v2
```

Note that the `-n` flag is specified. This prevents the tape drive from being rewound before the backup begins, enabling this backup to be “stacked” on the end of the previous backup image.

3. To initiate a pull backup of the `/home` filesystem on host *lasher*, from host *sysback1*, and send the data to `rmt1` of the host *sysback1*, type the following from *sysback1*:

```
mklvback -U lasher -f /dev/rmt1 /home
```

4. To initiate a pull backup of the `/home` filesystem on host *lasher*, from host *sysback1*, and send the data to `rmt1` of the host *shappy*, type the following command from *sysback1*:

```
mklvback -U lasher -h shappy -f /dev/rmt1 /home
```

Related Information

The `sysrestore`, `cfgremsvs`, `cfgremaccess`, `mkvginfo`, `cfgremrootaccess`, and `editlvminfo` commands.

Purpose

Creates or updates boot images on the server for booting network clients.
Configures the server to enable network booting of client machines.

Syntax

```

>>>mksbnetboot--B--h--"hostname"----->
|
|--a--"address"-----|
|--d--"net device"----|
|--g--"gateway"-----|
|--s--"subnet"-----|
|--u-----|
|--S--"server addr"---|
|--T--"platform"-----|
|--k--"kernel"-----|
|--n--"NIM SPOT"-----|
|--I--"NIM LPPSOURCE"---|
|--D-----|

```

Description

The **mksnetboot** command configures network boot clients and the boot images required to boot them. Both NIM Resource and Classic methods are handled. See Chapter 13, “Network Boot/Installation Configuration”, on page 13-1 for an explanation of NIM Resource and Classic netboot methods.

A boot image is created when a new client is configured. Boot images might need to be updated if any server software is updated. For example, if the NIM spot has a new software level applied to it, the corresponding boot images built from that spot should be updated.

For the Classic netboot method, the boot images should be updated if any software is applied to the netboot server (its /usr filesystem). The default case is to update all known boot images if an update is requested.

Configuring a Network Boot Client Machine

Classic Method: Specifying the **-h**, **-a** and **-d** arguments generates the information needed to respond to the client's BOOTP request and assigns the client the specific boot image used to boot the client, depending on the client's machine type. However, if you do not specify the **-a** option, the command requires, at a minimum, the **-S**, and optionally the **-s**, and **-g** flags to add a client using this method.

You only need to run this command for clients who will *boot* from the server. For clients that will boot from other media, such as installation diskettes or tape but will only install from this server, you do not need to run this command.

If the network adapter has been changed in the client system, you might need to update the server to reflect the new hardware address of the client machine. You can update the boot client information if already configured by following the same steps as for a new client. This overwrites the previous information.

NIM Method: When you add a network boot client that uses NIM resources, the **-d**, **-T**, **-k**, **-S**, **-s**, **-g**, and **-a** flags are not valid. The information that would be contained in these flags is contained in the NIM resource definition for the client. The required flags to add a NIM Resource Network Boot client are **-h**, **-n**, and **-l**.

Rebuilding Existing Network Boot Images

If you update or install software on the boot source, you must also update the boot image. For the Classic boot method, the boot source is the **/usr** directory of the boot server. For the NIM Resource Network Boot, the boot source is the NIM **SPOT** resource.

To rebuild the boot image for either method, use one of the following commands. To rebuild all existing boot images, type:

```
mksbnetboot -B ALL
```

To rebuild a specific build image, type:

```
mksbnetboot -B <image name>
```

A Note about the Network Hardware Address

The **-a** flag is used to specify the adapter “hardware” address, which differs for each adapter manufactured. The adapter address is needed by the server before it can respond to BOOTP requests. If you do not know the client network adapter hardware address, follow the instructions in “Determining the Network Adapter Hardware Address” on page B-5.

Enter this parameter only for **PCI-based RISC System (rspc)** clients, or if you want the client to boot using a *broadcast* BOOTP request. By entering the adapter hardware address for a non-rspc client, that client can be booted without filling out the server information in the BOOTP screen at system startup. This is accomplished by sending a broadcast BOOTP request that the server responds to by identifying the hardware address of the client’s network adapter. This information is not used by non-RISC PC clients requiring a gateway to reach the server.

Flags

-a “address”

Specifies the adapter hardware address of your network adapter. Note that this is *not* referring to the Internet (IP) address, but the hardware adapter address. This information is required on **PCI-based RISC System (rspc)** clients and is not used by other clients requiring a gateway to reach the server.

-d “net device”

Specifies the name of the network adapter for the network the clients will be booted from. You can also specify a network adapter type of either *ethernet* or *token-ring* if a device of the client’s network adapter type does not exist on the server.

-g “gateway”

Gateway address the client must use to reach this server, if any.

-h “hostname”

Specifies the name of the host to which the boot image is to be assigned or the client to be removed from the network boot configuration.

-k “kernel”

Indicates the kernel type, either “up” for uniprocessors or “mp” for multiprocessors.

- u**
Specifies that the hostname is to be unconfigured as a network boot client.
- s "subnet"**
Subnet mask of the client. The default is 255.255.255.0.
- B**
Specifies to update a network boot image.
- n**
The name of the NIM spot. The **-n** flag implies NIM netboot mode and also requires the **-n** flag. Valid spot names can be discovered using the command **lsnim -t spot**.
- l** The name of the NIM lpp_source. The **-l** flag also requires the **-n** flag. Use the command **lsnim -t spot** to find valid lpp_source names.
- S "server addr"**
IP address of the server. The default is the primary IP address of the current system. Specify this value only if the server has multiple IP addresses. Specify the address the client will use to contact the server.
- T "platform"**
The platform type of the client. Use the **-k** kernel flag to indicate the kernel type.

The following platform types are currently supported:
 - rs6k** Classic RISC System/6000
 - rspc** PCI-based (PC) RISC System/6000
 - chrp** Common Hardware Reference Platform
- D**
Indicates to build the network boot image with the AIX Kernel Debugger enabled. Use this flag for diagnostic purposes only. To use this flag, you must have a terminal attached to the machine's s1 port in order to interact with the kernel debugger to initiate the network boot. It is important to note the diagnostic value that is provided at the end of the boot image build. This alphanumeric word is a storage address used by the debugger at boot time.

Examples

1. To add a network boot client named "mars" and create a network boot image for a Multiprocessor RISC System/6000 platform on a token ring network using the Classic netboot method, type:
`mksbnetboot -h mars -T rspc -K up -d token ring -S 9.19.134.93`
2. To add a network boot client named "lasher" using the NIM resource method with a NIM **SPOT** called "spot_aix433" and an **LPPSOURCE** called "lpp_aix433", type:
`mksbnetboot -h laher -n spot_aix433 -l lpp_aix433`
3. To rebuild all previously configured network boot images, type:
`mksbnetboot -B all`

Files

/etc/bootptab	Contains entries for response to BOOTP requests received from the network.
/tftpboot/hostname	A symbolic link to an actual network boot image file for the specific hostname.

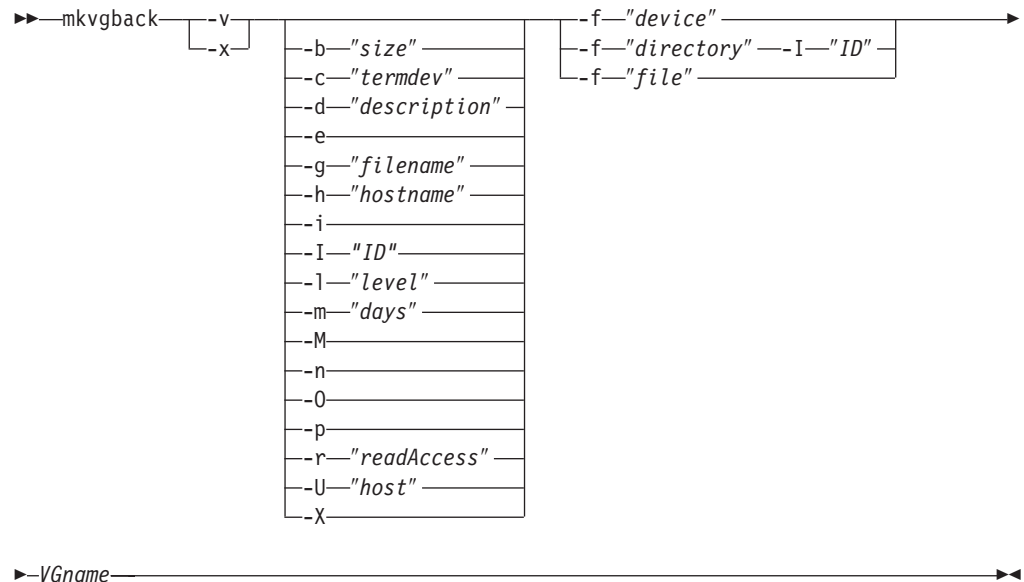
/usr/lpp/sysback/netinst/boot Directory where the actual boot images are stored.

mkvgback

Purpose

Performs a backup of one or more volume groups.

Syntax



Description

The **mkvgback** command is used to find and back up all files belonging to the specified volume group or groups.

The backup can be performed to a tape drive, virtual device, or disk image file. When specifying a disk image file, you can enter the full pathname of the file to create or overwrite. When doing so, the filename must begin with the prefix “VG” to indicate the file is a volume group backup. You can also specify only the backup directory and a *unique ID*. When doing so, a filename will be created for you. Refer to “Backups to Disk Image Files” on page 2-6 for information on the filename created. If you are creating a file and a file by the same name already exists, specify the **-O** option to overwrite the existing file.

The backup can also be performed to a remote device, virtual device, or disk image file. If *Remote Services* has been configured on both the local and server system using the **cfgremsvs** command, and you have defined a backup device on the server for use by this system using the **cfgremaccess** command, then you can also select a hostname using the **-h** option. The backup will then be written to the device or filename on the specified server, provided the server has enabled this system access to the specified device or directory.

The **-l level** option indicates that an incremental backup will be performed.

A level 0 backup must be performed before any level 1-9 can be performed. Refer to “Understanding Incremental Backups” on page 4-1 for additional details on incremental backups.

Files, or files within directories, that are specified in the exclude list will not be backed up with this command. See the **chexcludelist** command for information on creating exclude lists.

The backup can also be performed as a “pull” backup to enable central management of backups. The machine that “pulls” the backup is called the “initiator,” while the machine that is backed up is called the “backup system.” The machine that receives the backup data is called the “destination system.”

The initiator is the machine where the **mkdirback** command is issued. The backup system is referenced in the command syntax by the **-U “host”** flag. The data destination system is referenced by the **-h “host flag.”**

When only the **-U “host”** flag is specified, the **-f “device”** flag refers to a device on the initiator system. In this case, the backup destination and the initiator are the same system. This is known as a “two-way pull backup.”

When the **-U “host”** and **-h “host”** flags are specified, the **-f “device”** flag refers to a device on the host specified by the **-h “host”** flag. In this case, the backup destination and the initiator are different systems. This is known as a “three-way pull backup.”

Remote Services must be configured, using the **cfgremsvs** command, on all of the machines involved in the backup operation, the initiator, the backup system, and the data destination machines. The backup destination machine must have the Server Options of Remote Services configured to allow the backup system machine to send its data to devices on the backup destination machine. You can do this with the **Add or Change Client Host Access to this Server** option or the **cfgremaccess** command.

The backup system machine must have the Client Options of Remote Services configured to specify the backup destination machine as a backup host. You can do this with the **Add or Change List of Remote Backup Servers** option or the **cfgremserver** command.

The backup system must also configure Remote Command Access to allow the initiator machine to pull the backup.

Flags

-b “size”

Specifies the buffer size in K-bytes (1024-bytes). This value either increases or decreases the amount of data that is written to the output device at one time. Some devices with small buffers might require you to reduce this value, while other devices with very large buffers can benefit from increased performance by increasing this value. If you are unsure, use the default value (64 Kbytes).

-c “termdev”

If the backup spans multiple tape volumes, the volume prompt is sent to the *termdev* device (such as */dev/tty0*). If the **-h hostname** option is specified, this flag specifies the device on the remote host.

-d “description”

A custom description to be included in the backup header. If the description includes spaces, the entire description must be enclosed in double quotation marks (“”).

- e Forwards the tape to the end of the last Sysback backup. Used when stacking multiple backup images on a tape.
- f **"device, file or directory"**
Specifies the output device name, filename, or directory for the backup. The specified output option can be on the local system or server (if **-h** option provided). The device name can be a tape drive or virtual device name. If you specify a directory, you must also specify an *ID* using the **-I** flag.
- g **"filename"**
Indicates the name of an *LVM Information File* previously created and customized for this backup. Refer to the **mkvginfo** and **editlvminfo** commands.
- h **"hostname"**
Name of the remote backup server host to receive the backup data (such as the data destination host). This is the host that provides the backup device specified by the **-f** flag.
- i Indicates to dynamically create a backup file ID when writing backups to disk image file. This flag supersedes the **-I"ID"** flag.
- I **"ID"**
This option is used only if a directory is specified as the output device. The ID is included in the filename created to make it unique from other disk image file backups. If a backup in the same directory with this ID already exists, specify the **-O** flag to overwrite the previous backup.
- l **"level"**
Specifies the backup level (default is 0, or all files). Valid values are 0-9. Only files created or changed since the last (*level - 1*) backup was performed.
- M
Retains physical partition mapping, by default, when the logical volume is recreated from this backup. Unless the logical volume was originally created using a physical partition map, it is generally recommended that it not be recreated using the same partitions, as this would preserve fragmentation that develops over time as logical volumes and filesystems are expanded. You can specify whether or not partition mapping will be used before recreating the logical volume.
- n
Indicates that the tape should not be rewound at the beginning of the backup. This enables the backup to be appended to the previous backup performed. The tape is not automatically rewound at the end of the backup. The **-n** option is always ignored when backing up to a non-tape device.
- O
Overwrites the previous file, if a filename was specified as the output device, and the filename already exists.
- P
Indicates that the data should be packed before being written to the media. This typically reduces size of backup between 25% and 40%. For increased performance, do not use this option when backing up to a device that provides hardware data compression.
- r **user=[u | a]**
Specifies user read permission when backing up to a disk image file. **"u"** indicates only the specified user can read the file. **"a"** indicates that any user can read the file.

-r host=[h | a]

Specifies host read permission when backing up to a disk image file. “h” indicates only the specified host can read the file. “a” indicates that any host can read the file.

-U “host”

Name of the host to be backed up (such as the backup system).

-v Specifies that file names should be listed on the screen as the files are being backed up. This flag cannot be used with the **-x** flag.

-x Specifies that the progress indicator should be shown on the screen, displaying the approximate size and time to read the entire contents of the media and the amount completed. This flag cannot be used with the **-v** flag.

-X

Excludes all non-JFS (journaled file system) logical volumes, or “raw” logical volumes, from the backup.

Examples

1. To perform a level 1 backup of the *vg00* volume group to the directory */usr/lpp/sysback/bf/saturn/root*, listing the files as they are backed up, type:

```
mkvgback -vf /usr/lpp/sysback/bf/saturn/root -I vg00_lev1 -l1 vg00
```

The file created will be

/usr/lpp/sysback/bf/saturn/root/VG.hostname.vg00_lev1.

2. To perform a remote backup to the virtual device *vdev3* on the host *jupiter* that is a compressed backup of the *uservg1* and *uservg2* volume groups and to display a progress indicator, type:

```
mkvgback -pxh jupiter -f vdev3 uservg1 uservg2
```

3. To perform a remote backup to the virtual device */dev/rmt1* of the *data1* volume group, including only the files created or changed in the last two days, type:

```
mkvgback -nf /dev/rmt1 m2 data1
```

4. To initiate a pull backup of the */home* filesystem on host *lasher*, from host *sysback1*, and send the data to *rmt1* of the host *sysback1*, type the following from *sysback1*:

```
mkvgback -U lasher -f /dev/rmt1 /home
```

5. To initiate a pull backup of the */home* filesystem on host *lasher*, from host *sysback1*, and send the data to *rmt1* of the host *shappy*, type the following command from *sysback1*:

```
mkvgback -U lasher -h shappy -f /dev/rmt1 /home
```

Related Information

The *sysrestore*, *cfgremsvs*, *cfgremaccess*, *mkvginfo*, *cfgremrootaccess*, *editlvminfo* and *chexcludelist* commands.

mkvginfo

Purpose

Generates information needed in recreating volume groups and logical volumes from backups.

Syntax

```
➤ mkvginfo [-f] [-M] [-o "filename"] [-v VGname] [-l LVname] ➤
```

Description

The **mkvginfo** command is automatically executed by each SysBack backup command that stores LVM information on the backup. This information contains the volume group, logical volume, filesystem, and physical volume attributes that can be later used to recreate any of the preceding from the backup media.

The arguments supplied to the command and the resulting output depend on the type of backup performed. This command sends the results to standard output (stdout) by default, unless the **-o filename** option is specified.

This command generates LVM information for either a list of volume groups, if the **-v VGnames** option is specified, or for a list of logical volumes if the **-l LVnames** option is specified. If the logical volumes contain filesystems, the filesystem attributes are recorded as well.

The output contains a label, indicating the record type, followed by the attributes for the particular label. The contents of the **/etc/filesystems** file, for the logical volumes involved, are appended to the end of the file.

The information contained in the output is as follows:

System Information (one of each of the following):

TYPE	Backup type (VG, LV, SYSTEM, POWER)
VERSION	Version and Release of AIX (such as "4.1")
PLATFORM	Platform Type (such as rs6k)
KERNEL	Kernel Type (up/mp)
SBVER	SysBack Version, Release and Modification Level (such as 040101)

Table of contents (one record, indicates volume group data, if any, included on backup):

TOC	Static Header
vgname(s)	List of volume groups (separated by spaces)
x	Static Trailer

Physical Volumes (one record for each):

PV	Static Header
PVid	Physical volume ID

Physical Volumes (one record for each):

Location	Location Code (address)
Hdiskname	Hdisk Name (not used)

Volume Groups (one record for each):

VG	Static Header
vname	Volume Group name
autoon	Auto varyon at system startup? (Y/N)
ppsize	Physical partition (in MB)
vgopt	[C]reate/[I]mport/[X]gnore
quorum	Are quorums active? (Y/N)
concurrent	Concurrent-capable? (y/n)
autoconc	Auto-Concurrent Varyon? (y/n)
pvlst	List of physical volume IDs

Logical Volumes (one record for each)

LV	Static Header
priority	(01=mapped, 02=striped, 03=boot, 04=jfslog, 10=paging, 20=jfs, 90=dump)
mountpt	Filesystem mount point or '-' if not jfs
vname	Volume group name
lvname	Logical volume name
type	Logical volume type (see priority)
createopt	Create this LV? (Y/N)
origmb	Original size in MB
lps	Size to create in LPs (can change by user)
copies	Number of copies (#PPs per LP)
minips	Minimum LPs to contain filesystem data (1 if not jfs)
intra	Intra-pv allocation policy (ie/im/c/om/m/oe/e)
inter	Inter-pv allocation policy (m/x)
upper	Upperbound - Max PVs if maximum inter policy
mzxlps	Maximum LPs for this LV
mwc	Mirror-write-consistency on? (y/n)
bbpolicy	Bad block relocation? (y/n)
relocatable	Can LV be relocated? (y/n)
strict	Can multiple copies be place on one PV? (y/n)
verify	Write verify? (y/n)
stripesz	Stripe Size
stripewd	Stripe width
ppmap	Create using physical partition map? (y/n)
LVpvlst	Physical volume IDs

Filesystems (JFS only - one record for each) – AIX Version 4 only:

FS	Static Header
mountpt	Mount point (same as in LV record)
vname	Volume Group name
lvname	Logical Volume name
fragsize	Fragment Size
nbpi	Number of bytes per inode
compress	Compress? (LZ, no)
bfsupport	Big File Support? (y/n) (AIX 4.2+)

Filesystems (JFS only - one record for each) – AIX Version 4 only:

agsize	Allocation Group Size (#MB) (AIX 4.2+)
--------	--

Physical Partition Maps (one or more each logical volume – each not to exceed 50 PPs):

PP	Static Header
lvname	Logical Volume name
ppno:ppvid	Physical partition number: physical volume ID (one for each PP in the LV)

Filesystem stanzas (one record for each):

Stanza taken directly from `/etc/filesystems` file

The information produced by this command is placed on the beginning of each backup and can be read from the backup using the **sbread** command with the **-T** flag.

Including a customized LVM information file on a backup: You can create and customize an LVM information file to be included on a SysBack backup. This information enables you to later recreate volume groups, logical volumes, or filesystems using the customized attributes without requiring the user to make the changes manually using the menu options.

To do so, use the following steps:

1. Use the **mkvginfo** command to create an LVM information file. Use the **-o filename** option to specify an output filename.
2. Use the **editlvminfo** command to edit the file using the menus and options described in Chapter 11, “Changing the Volume Group, Logical Volume and Filesystem Attributes”, on page 11-1.
3. Create the backup using the **mkjfsback**, **mklvback**, **mkvgback** or **sysback** commands. Use the **-g filename** option with the command to include the customized file instead of generating a new one.

Flags

- f** Indicates the command should continue even if filesystems are not mounted. Ordinarily, this command fails if a filesystem is not mounted.
- l** Indicates that a list of logical volumes is supplied and that the LVM information should be generated only for the specified logical volumes and filesystems, if applicable.
- M**
Indicates that the default when recreating the logical volume or logical volumes is to recreate using physical partition maps. If not specified, the default is to recreate the logical volumes using contiguous partitions on the physical volumes, whenever possible.
- o “filename”**
The name of the file where the output should be sent. If not specified, output is sent to standard output.
- v** Indicates that a list of volume groups is supplied and that the LVM information should be generated for the specified volume groups.

Files

/etc/filesystems	Contains filesystem stanzas that are copied to the output of this command for each logical volume containing a filesystem.
-------------------------	--

Related Information

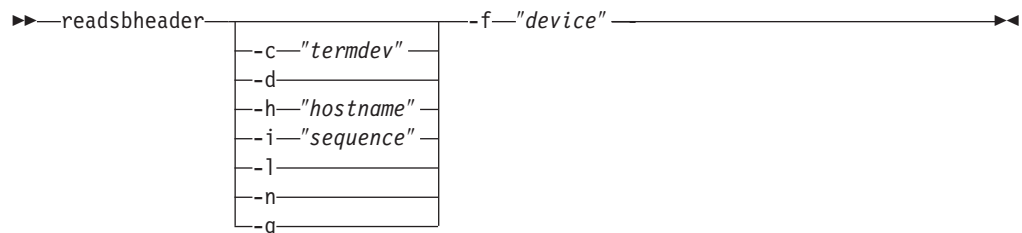
The **mkjfsback**, **mklvback**, **mkvgback**, **sysback**, **editlvminfo** and **sbread** commands.

readsbheader

Purpose

Reads the header label on any SysBack backup.

Syntax



Description

The **readsbheader** command can be used to read the header information on any SysBack backup. It can be used to list the general header information, the list of images (logical volumes and filesystems) included on the backup, and the list of files and directories included on the backup. This command is useful for reading the contents of an unknown backup tape when no printed label was affixed.

If the backup media is a tape that contains multiple backups, you can read the header information from any backup on the tape by using the **-i "sequence"** option. The sequence refers to the backup sequence number, "1" being the first backup on the tape and so on.

Flags

-c "termdev"

If the backup contains multiple tape volumes, the volume prompt is sent to the display indicated by "termdev" (such as /dev/tty0 or /dev/lft0). If the **-h "hostname"** option is specified, this flag specifies the display on the remote host.

-d

Indicates that a list of logical volumes and filesystems included on the backup should be displayed also.

-f "device or file"

Tape device, virtual device, or filename containing the backup. If a filename is specified, the information is read from the file on the disk with the **".TOC"** extension. You do not need to supply this extension.

-h "hostname"

Hostname of backup server to which the remote backup device is attached.

-i "sequence"

Indicates the backup sequence number to read. "1" refers to the first backup on the tape, and so on. The default is "1." This option can be specified only when reading from a tape drive or virtual device.

-l

Indicates that a list of files and directories included on the backup should be displayed. This file list can be very long. The directories are listed first, followed by the regular files.

-n

Indicates that tape drives should not be rewound prior to reading. This assumes that the tape drive is already positioned at the beginning of the backup to read.

-q

Indicates that no status messages should be displayed while searching and reading the backup media.

Examples

1. To show the general header information on a backup in tape device */dev/rmt0*, on host *mars*, type:
`readsbheader -f rmt0 -h mars`
2. To read the contents of the third backup on virtual device *vdev2*, including the list of logical volumes, filesystems, directories and files on the backup, type:
`readsbheader -dli3 -f vdev2`

Related Information

The **sbread** and **sbwrite** commands.

remakevg

Purpose

Recreates one or more specified volume groups, logical volumes, or filesystems from LVM information contained on the backup media.

Syntax

```
►—remakevg—┬──c—"termdev"—┬──f—"device"—┬──v—VGname—┬──l—LVname—►
              └──E—┘
              └──n—┘
              └──h—"hostname"—┘
              └──i—"sequence"—┘
              └──L—"LVname"—┘
              └──q—┘
              └──V—"VGname"—┘
```

Description

Use the **remakevg** command to recreate one or more volume groups, logical volumes, or filesystems using information contained on any backup type except for the file/directory backup. A volume group, logical volume, or filesystem can only be recreated from a backup containing the specified data, unless the backup is a system backup, which contains the information needed to recreate any volume group, logical volume, or filesystem regardless of the data included on the backup.

After the LVM information is read from the backup, a verification ensures that the correct physical volumes and space are available to create the volume group and logical volumes. If not, you will be required to change the LVM information to satisfy the space requirements.

If the verification fails, or if the **-E** flag is specified, a user-interface enables you to view or change the LVM information before the volume groups, logical volumes, or filesystems are created. Refer to Chapter 11, “Changing the Volume Group, Logical Volume and Filesystem Attributes”, on page 11-1 for details on changing the LVM information.

If the **-E** option is not specified, and there are no problems detected when verifying the consistency between the LVM information and the current system configuration, the volume groups, logical volumes, and filesystems are recreated without additional user-interaction. However, unless the **-q** option is provided, you will be asked to confirm before any recreation takes place.

Note that this command recreates only the specified volume groups, logical volumes, and filesystems (if applicable). It does not restore the data from the backup media. After creating the desired volume group, logical volume, or filesystem, you can restore the data with the **sysrestore** command.

Flags

-c "termdev"

If the backup contains multiple tape volumes, the volume prompt is sent to the

display indicated by “termdev” (such as /dev/tty0 or /dev/lft0). If the **-h** “hostname” option is specified, this flag indicates the display on the remote host.

-E

Displays the user-interface menus to enable the LVM information to be changed before the volume groups, logical volumes, or filesystems are created.

-f “device or file”

Tape device, virtual device, or filename containing the backup. If a filename is specified, the information is read from the file on the disk with the “.TOC” extension. You need not supply this extension of the filename.

-h “hostname”

Hostname of backup server to which the remote backup device is attached.

-i “sequence”

Indicates the backup sequence number to read. “1” refers to the first backup on the tape, and so on. The default is “1”. This option can be specified only when reading from a tape drive or virtual device.

-l Indicates that logical volumes (and filesystems, if applicable) should be created and that the logical volume list is provided at the end of the command.

-L “LVname”

To recreate a logical volume under a different name, specify the new LVname. This enables you to recreate the logical volume even if the original still exists on the system. This flag is applicable only when recreating a logical volume, and you can only specify one logical volume name to create when using this flag.

-v Indicates that volume groups should be created and that a list of volume groups is provided at the end of the command.

-V “VGname”

If creating a single volume group: To recreate the volume group under a different name, specify the new VGname. This enables the volume group to be created even though the original still exists.

If creating a logical volume: Indicates the volume group name the logical volume will be created in. Used to move a logical volume from one volume group to another.

-q

Specifies that no status messages should be displayed while reading the information from the backup media.

-n

Specifies that the tape is already positioned at the beginning of the select volume group (on stacked tapes).

Examples

1. To recreate a volume group from a backup on tape device /dev/rmt0, previously called *uservg*, under the new name *newuservg*:
remakevg -f /dev/rmt0 -v -V newuservg uservg
2. To recreate the *lv00* and *lv01* logical volumes from a volume group backup image file on host *venus*, placing the logical volume in volume group *vg01*, type:
remakevg -l -h venus -V vg01 -f \
/usr/lpp/sysback/bf/VG.saturn.12300200 lv00 lv01

3. To recreate the *datavg1* and *datavg2* volume groups from the backup on virtual device *vdev0*, enabling the user to change the LVM information prior to the creation, type:

```
remakevg -Ev -f vdev0 datavg1 datavg2
```

Related Information

The **sysrestore** command.

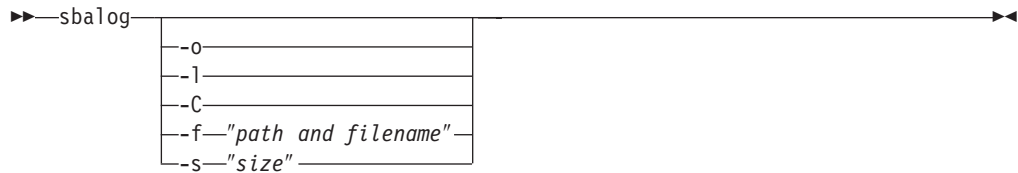
Chapter 11, “Changing the Volume Group, Logical Volume and Filesystem Attributes”, on page 11-1.

sbalog

Purpose

Changes, lists, or displays the SysBack log.

Syntax



Description

The SysBack log file provides a mechanism to track the completion status of SysBack backup, restore, and verify operations. For information about the SysBack log file, see Chapter 19, “Activity Logging”, on page 19-1.

Flags

- o Lists the contents of the SysBack log file.
- l Displays the current size and location of the SysBack log file.
- C Changes the size or location of the SysBack log. You must use either the -f or -s flag with this flag.
- f “**path and filename**” Specifies the location of the SysBack log. Used with the -C flag.
- s “**size**” Specifies the size of the SysBack log in multiples of 4096 Kbytes.

Examples

1. To change the SysBack log location to **/tmp/logs/sysback.log**, type:
sbalog -C -f /tmp/logs/sysback.log
2. To change the size of the log to 8192 Kbytes, type:
sbalog -C -s 8192
3. To change the size and location of the log, type:
sbalog -C -f/tmp/logs/sysback.log -s 8192
4. To list the contents of the log, type:
sbalog -o

Files

/var/adm/ras/sysback.log
The default SysBack log file.

Related Information

The **cfgremsvs**, **cfgremaccess**, **sbread**, **sbwrite**, and **cat** commands.

sbclient

Purpose

Performs all SysBack remote command execution.

Syntax

```
➤—sbclient—-i—hostname  
IPaddress—command-argument—➤
```

Description

The **sbclient** command is used to execute all remote commands in SysBack. It can be used only after Remote Services has been configured on the local and remote system using the **cfgremsvs** command, and the remote system has granted permission to the local user and host to perform remote commands using the **cfgremaccess** command.

When **cfgremsvs** command is run, a user called *sbnet* is created. All remote commands are executed under this user. There is no need for the username on the local system to exist on the remote system for the local user to execute remote commands. The *sbnet* user must have UNIX file permissions to access any devices or directories that any remote user will need to write to.

To specify the remote hostname on which the command will be executed, you can specify either a hostname or an IP address. The hostname might require the full domain name to reach the remote host.

Only commands that are specified in the **remote_cmds** file on the server can be executed remotely. Any attempt to execute a remote command not defined in this file will fail.

The **-i** flag indicates that the command should read standard input from the user or that standard input will be piped to the remote command from a local command. If the **-i** flag is not specified and input is requested from the remote command, the command locks up indefinitely. The **-i** flag can be specified, however, even if no input is requested, but performance might be affected.

The **sbclient** command causes the **sbserver** command to be executed on the remote system. The **sbserver** command is a daemon that establishes the socket connection with the local system, sets environment variables, executes the specified command, reads input, and writes output to the socket.

In addition to the standard environment variables used for login users, the following environment variables are automatically set on the remote system before the remote command is executed:

CLIENT_BDIRS

Specifies one or more backup directories, separated by colons, as defined in the **.remote_access** file, to which this host and user can read or write.

CLIENT_DEVS

Specifies one or more devices, separated by colons, as defined in the **.remote_access** file, to which this host and user can read or write.

CLIENT_HOST

Hostname or full domain name (if required) of client host performing the command.

CLIENT_HOSTPERM

Indicates the hostname, as it appears in the **.remote_access** file, that granted permission to the client. This can be the client hostname, the full domain name of the client, or *all*.

CLIENT_IDIRS

Specifies one or more installation image directories, separated by colons, as defined in the **.remote_access** file, to which this host and user can read or write.

CLIENT_IPADDR

IP address of the client host performing the command.

CLIENT_USER

User name on the client host performing the command.

CLIENT_USERPERM

Indicates the user name, as it appears in the **.remote_access** file, that grants permission to the client. This is either the same as *CLIENT_USER* or *all*.

The above environment variables can be accessed by the remote applications running on the server and can also be queried from the client using a command such as:

```
sbclient Remotehost echo \${CLIENT_DEVS}
```

Flags

- i Indicates the remote command must receive standard input from the local system. Use this flag only when executing an interactive command or piping data to the command.

Examples

1. To read the header of a remote backup tape in device */dev/rmt0* on host *saturn*, type:

```
sbclient saturn sbread -H /dev/rmt0.1
```
2. To copy the file **/tmp/imagefile** to the remote host *neptune*, type:

```
cat /tmp/imagefile | sbclient -i neptune \  
"cat > /tmp/imagefile"
```

In this example, the local file **/tmp/imagefile** is sent as input to the **sbclient** command. The **cat** command is executed on the remote system, which copies the data received into a new file **/tmp/imagefile**. Note that the new file on the server will be owned by the *sbnet* user ID.

Files

/usr/lpp/sysback/.remote_access

Contains list of hosts and users that are allowed to execute commands on the local system.

/usr/lpp/sysback/.remote_cmds

Contains list of commands that can be remotely executed on the local system.

Related Information

The `cfgremsvs`, `cfgremaccess`, `sbread`, `sbwrite`, and `cat` commands.

sbcomp and sbuncomp

Purpose

Compresses and decompresses data respectively.

Syntax

►►—sbcomp—◄◄

►►—sbuncomp—◄◄

Description

The **sbcomp** command compresses data from standard input and sends the resulting compressed data to standard output. The **sbuncomp** command uncompresses data from standard input and sends the resulting decompressed data to standard output.

The **sbcomp** and **sbuncomp** commands are used as filters and use only memory to perform the compression or decompression (there is no intermediate file storage used). Performing software compression and decompression uses a great deal of CPU resource and can affect the overall performance of the system. If the data is to be written to a hardware device that performs its own compression, do not compress the data before writing to the media, as this uses CPU resources unnecessarily.

If you select to compress data before writing to media when performing any SysBack backup command with the **-p** flag, the resulting backup data is piped through the **sbcomp** command before sending it to the **sbwrite** program, which places the data on the output media. The SysBack restore commands always read the backup header to determine if the data on the backup was compressed using **sbcomp**, and then pipe the data output by **sbread** to the **sbuncomp** program before the data is restored to disk.

Flags

None.

Examples

1. To compress data in the file **/data** and send the results to **sbwrite** to write to the tape drive **/dev/rmt0**, type:

```
cat /data | sbcomp | sbwrite -Svp -tl -nrawlv /dev/rmt0
```
2. To decompress and restore the file **/data** from the backup performed above, type:

```
sbread -Sv /dev/rmt0 | sbuncomp > /data
```

Related Information

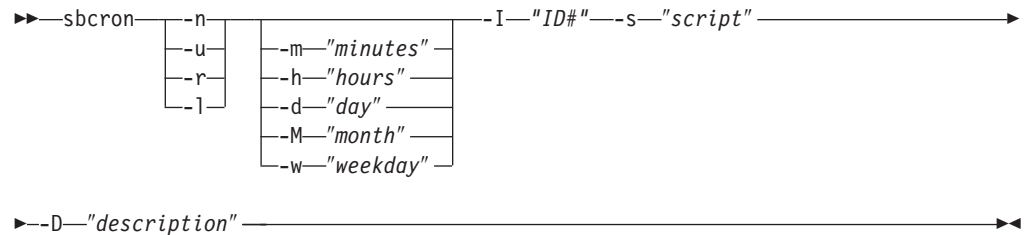
The **sbread** and **sbwrite** commands.

sbcron

Purpose

Adds, updates, lists, or removes a regularly scheduled command.

Syntax



Description

The **sbcron** command is used to add, update, list, or remove a regularly scheduled command. Regularly scheduled commands are scheduled using one or more of the following flags: **-m**, **-d**, **-M**, or **-w**.

The following rules apply to this command:

- You must use a whole number for the **-m**, **-h**, **-d**, **-M**, and **-w** flags.
- To indicate an inclusive range, use two numbers separated by a dash. For example, to schedule a command to run Tuesday through Friday, use the **-w** flag with a value of "2-5".
- To indicate that a script should be run on separate days (not an inclusive range), separate the numbers with a comma. For example, to schedule a command to run on the first and last day of January, use the following flags:

`-M 1 -d 1,31`

Note: Do not use a space after the comma.

- When you add or update a new entry (created using **-n**), you must use the **-m** and **-h** flags.
- If the **-d**, **-M**, or **-w** flags are omitted, all allowed values will be used in place of the missing flag. For example, to schedule a command to run at 6:30 AM every day of every month, use the following syntax:

`sbcron -s /vg_backup -m 30 -h 6`

To schedule a command to run at 6:30 AM every *Monday* of every month, use the following syntax:

`sbcron -s /vg_backup -m 30 -h 6 -w 1`

Flags

- n** Creates a new schedule for the script defined with the **-s** flag.
- u** Updates an existing schedule.
- r** Removes an existing schedule.

- l** Lists all scheduled SysBack scripts.
- m "minutes"**
Specifies the minutes for scheduling a script. Valid values are from 1 to 60.
- h "hours"**
Specifies the hour for scheduling a script. Valid values are 0 to 23, where 0 is equal to 12:00 AM, and 23 is equal to 11:00 PM.
- d "days"**
Specifies the day a script should be scheduled. Valid values are from 1 to 31.
- M "month"**
Specifies the month a script should be scheduled. Valid values are from 1 to 12, where 1 is equal to January, and 12 is equal to December.
- w "weekday"**
Specifies the day of the week a script should be scheduled. Valid values are from 0 to 6, where 0 is equal to Sunday and 6 is equal to Saturday.
- I "ID#"**
Specify the SysBack ID number of the script to remove.
- s "script"**
The script to be scheduled.
- D "description"**
Enables you to include a custom description. This description is included in the list created using the **-l** flag.

Examples

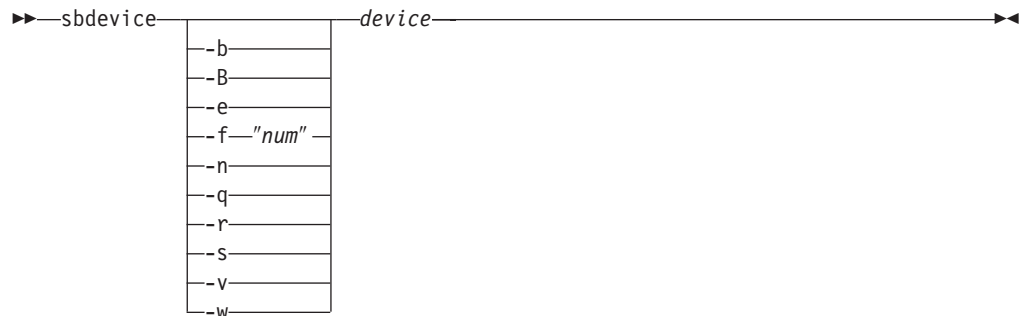
1. To schedule the **vg_backup** script:
`sbcron -m 0 -h 23 -w 1-5 -s /scripts/vg_backup`
2. To schedule the **system_backup** script to run at 12:00 AM on the first, fifteenth, and thirtieth of each month:
`sbcron -m 0 -h 0 -d 1,15,30 -s /home/scripts/system_backup`
3. To schedule the **fs_backup** script to run at 6:30 AM every Monday, Wednesday, and Friday:
`sbcron -m 30 -h 6 -w 1,3,5 -s /fs_backup`
4. To schedule the **system_backup** script to run every day at 12:00 AM:
`sbcron -m 0 -h 0 -s /system_backup`
5. To remove the schedule with an ID of SB102:
`sbcron -r -I SB102`
6. To obtain a listing of schedules:
`sbcron -l`

sbdevice

Purpose

Checks tape drive availability and controls tape movement.

Syntax



Description

The **sbdevice** command is used to check the availability of the specified tape drive or drives and to perform other tape commands. Either tape drive names or a virtual device name can be specified for the *device* parameter.

For tape devices, you only need to specify the base device name (for example, *rmt0*). The tape will not be moved unless rewinding, forwarding, or backspacing, regardless of the tape device names or virtual device name specified.

Flags

- b**
Causes a tape drive or virtual device to back up a file mark. If the drive is at the beginning of a backup image, it will be positioned at the start of the previous backup image. If the drive is currently within a backup image, it will be returned to the start of the current image.
- B**
Reads and returns the current block size of the tape drive. A value of 512 is returned for all other device types.
- e** Rewinds and *ejects* tapes from the specified drives. If a sequential autoloader is used, the next sequential tape is inserted automatically.
- f "num"**
Forwards the tape past the specified "num" number of file marks. This is used to position to the next backup image on the tape.
- n**
Indicates that the program is to exit with an error code if any errors should occur. The default action is to display a message on most errors and wait for the tape to reset.
- q**
Indicates that no errors should be displayed. The command exits with a non-zero return code if an error occurs.
- r** Rewinds the specified device or devices.

- s Checks if the tape drive is currently at the beginning of the tape. Return code of 0 indicates the tape is not rewound; 1 indicates the tape is rewound.
- v Indicates that messages (such as *"Rewinding /dev/rmt0 ..."*) should be displayed as operations are performed on each tape drive.
- w Indicates that the device or devices should be checked for write permission. For tapes, the write-protect switch is checked and an error is returned if it is set. For files, an error is returned if the user does not have write permission to the file or directory.

Examples

1. To read the current block size of tape drive */dev/rmt0*, type:
`BS=vsbdevice -B rmt0v`
2. To rewind and eject all tapes from drives included in the *vdev0* virtual device, showing messages as the drives are rewound, type:
`sbdevice -ve vdev0`
3. To only check for write permission to the file or directory ***/usr/lpp/sysback/images/venus.rootvg.01201244:***
`sbdevice -w /usr/lpp/sysback/images/local/VG.venus.01201244`
4. To rewind device */dev/rmt0* and */dev/rmt1*, indicating that the command should not wait if an error occurs, type:
`sbdevice -nr rmt0 rmt1`

sbejecttape

Purpose

Used to eject either a local or remote tape drive or SysBack virtual device.

Syntax

```
►►—sbejecttape—f—"device"—h—"hostname"—◄◄
```

Description

Use this command to eject a tape from a local or remote tape drive or from a SysBack virtual device.

Flags

-f "device"

Specifies the output device name. The device can be a tape drive or a virtual device name and can be located on the local system or a server (if the **-h** flag is also used).

-h "hostname"

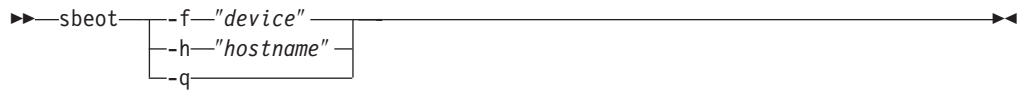
Specifies the remote tape server host to which the device is attached. This option is available only for remote backups after both the tape server and the local machine have been properly configured.

sbeot

Purpose

Forwards to the end of the data on a SysBack-created tape.

Syntax



Description

Use this command to forward to the end of the last backup on a tape created by one of the following SysBack commands: **sysback**, **mkvgback**, **mkjfsback**, **mkdirback**, **mklvback**. You can then append another SysBack backup to the end of the data on the tape.

The following restrictions apply:

- All the images on the tape must have been created by SysBack Version 4 or higher.
- The tape on which you want to append a backup must be loaded in the tape drive. For example, if the previous backup spanned three tapes, you must load the third tape into the tape drive before running the **sbeot** command.

Flags

-f "device"

Specifies the output device name. The device can be a tape drive or a virtual device name and can be located on the local system or a server (if the **-h** flag is also used).

-h "hostname"

Specifies the remote tape server host to which the device is attached. This option is available only for remote backups after both the tape server and the local machine have been properly configured.

-q

Suppresses the output. The command displays error messages if they occur.

Examples

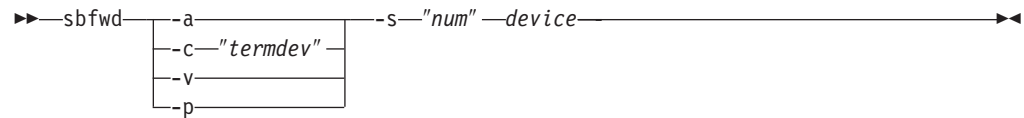
1. To position the tape to end of a local system and suppress progress of positioning:
`sbeot -qf /dev/rmt0`
2. To position the tape to end on a remote server:
`sbeot -h hercules -f /dev/rmt1`

sbfwd

Purpose

Forward one or more tape devices to a specific image.

Syntax



Description

The **sbfwd** command is used to forward a specified number of images to a tape or tapes written with the **sbwrite** program. **sbfwd** is a low-level command called by the SysBack restore programs when multiple backups are appended to the same media.

If a virtual device was used to perform the backup, you can omit the **-P** and **-a** options when specifying a virtual device name to forward. If a virtual device name was not used, and the backup being read was written with a *parallel* write-policy, specify the **-P** flag and include all devices in the list. If the backup was created with a *sequential* write-policy, you can list multiple device names, and the forwarding continues on the next sequential device when the first one reaches end of volume.

This command should be used only by experienced users who have created backups using the **sbwrite** command outside of the normal SysBack backup process.

Note: You must specify no-rewind tape device names (such as `/dev/rmt0.1`) with this command. Otherwise, the devices are automatically rewound when the command is complete.

Flags

- a** Indicates the device is an auto-loader. You are not prompted to change volumes, but the forwarding continues automatically when the next volume is inserted.
- c "termdev"**
If the backup contains multiple tape volumes, the volume prompt is sent to the "termdev" device (such as `/dev/tty0`).
- v** Indicates summary header information should be displayed as each image is read. This gives the header information of the image that is being skipped.
- P**
Indicates the backup was performed with a parallel write-policy, so all specified devices should be forwarded synchronously. If not specified, a sequential write-policy is assumed, and only the first device in the list is forwarded unless the end of media is encountered.
- s "num"**
Number of images (backups) to skip

Examples

1. To forward devices */dev/rmt0* and */dev/rmt1* in parallel to the third image (skipping 2 images), type:
`sbfwd -P -s2 rmt0 rmt1`
2. To forward virtual device *vdev0* to the next image, type:
`sbfwd -s1 vdev0`
3. To forward autoloader device */dev/rmt2* to the fifth image (skipping four images), showing the header on each backup image as it is passed, type:
`sbfwd -av -s4 rmt2`

Related Information

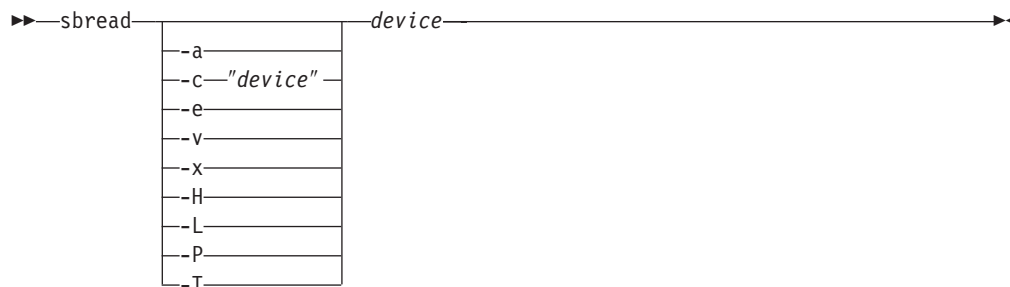
The **sbread** and **sbwrite** commands

sbread

Purpose

Reads data from all SysBack backup types.

Syntax



Description

The **sbread** command is used to read a backup that was created using the **sbwrite** command. All SysBack backups are written to the media using **sbwrite**, and all SysBack restore programs use **sbread** to retrieve the data from the media. In addition, SysBack uses **sbwrite** to store the table of contents (LVM information), file list, and other information identifying the type and contents of the backup. This information can then be retrieved using the **sbread** command.

The *device* parameter can be one or more tape drives, a virtual device, or a dash (-) indicating that the input should be received from standard input (*stdin*).

The **sbread** command reads data only from backup devices or directories to which the local host and user has access, as defined by the **cfglocaccess** or **cfgremaccess** commands. When **sbread** is executed locally, the access permissions are checked in the **.local_access** file. When executed by the **sbclient** command on a remote host, the remote host and user access permissions are checked in the **.remote_access** file.

By default, **sbread** assumes the data was backed up with **sbwrite** using a sequential write policy. If you used a virtual device name to perform the backup, you can use the same virtual device name to read the backup. Otherwise, if you are reading from a backup created with a parallel write policy, you must specify the **-P** flag to the **sbread** command. Also, when reading from a backup made using a parallel write-policy, you must also specify the same number of devices to read the data as was used to create the backup.

SysBack backups, with the exception of the raw logical volume backups, are formatted using either the AIX **backup** or **tar** command. The resulting data is sent to the **sbwrite** program, which stores the data on the media, including the backup header, table of contents (LVM and filesystem information) and file list, if specified. To read the same backup, it is necessary to use the **sbread** program to read the data from the media and send the results to the AIX **restore** or **tar** program to be unformatted and placed in the AIX filesystems.

When you use the **-H**, **-T**, or **-L** options with a no-rewind tape device name, the data is read from the beginning of the backup media and the tape is repositioned at the beginning of the same backup image. By omitting the **-H**, **-L** and **-T** flags, it

is assumed you are to read the actual data from the backup image. You can compress data before writing to the media. If compressed data is written to the media, the data must be uncompressed before it is restored to disk. The SysBack backup programs compress data using **sbcomp** and also indicate to **sbwrite** that the backup is compressed by using the **-p** flag. Before reading a backup with **sbread**, you can query whether the data was compressed by reading the backup header (**sbread -H**). If *Packed: Y* is shown, you should uncompress the data as it is output by **sbread** using the **sbuncomp** program.

If the data you want to read is not contained in the image the tape is currently positioned to, you must use the **sbfwd** command to forward the tape to the correct image before reading.

Flags

- a Indicates the device is an auto-loader. This flag suppresses the volume prompt, requesting that the user change tapes. Instead, a message indicates the tape is unloading and waiting for next volume. The reading continues automatically when the autoloader has inserted the next volume.
- c "**termdev**"
If the backup contains multiple tape volumes, the volume prompt is sent to the "**termdev**" device (such as `/dev/tty0`).
- e Indicates all devices (if tape) should be rewound upon completion. The default action is to not rewind.
- v Indicates whether status messages should be displayed at the beginning and end of the backup.
- x Displays the progress indicator when reading the data.
- H
Indicates the header information should be read from the backup. If using a no-rewind tape device, the tape will be repositioned to the beginning of the same image when completed.
- L
Reads the file list from the backup, if it exists. If using a no-rewind tape device, the tape is repositioned to the beginning of the same image when completed.
- P
Indicates the backup was performed with a parallel write-policy, so all specified devices should be read synchronously. If not specified, a sequential write-policy is assumed, and only the first device in the list is read unless the end of media is encountered.
- T
Reads the table of contents (LVM and filesystem information) from the backup, if it exists. If using a no-rewind tape device, the tape is repositioned to the beginning of the same image when completed.

Examples

1. To read the contents of a compressed sequential backup created using the **sbwrite** command to virtual device `vdev1`, saving the results in a file called `/tmp/file`, type:

```
sbread vdev1 | sbuncomp > /tmp/file
```

2. To read the header (label) on device */dev/rmt1* and to not rewind after reading, type:
`sbread -H rmt0`
3. To read the table of contents from the media, type:
`sbread -T rmt0 > /tmp/toc.out`
4. To read the data contained in the parallel backup of */dev/rmt0* and */dev/rmt1*, displaying the progress indicator as the backup is read, and sending the output to the AIX **restore** command to restore the data to the AIX filesystem, type:
`sbread -Px rmt0 rmt1 | restore -xvqf-`

Files

/usr/lpp/sysback/.remote_access

Contains list of hosts and users that are allowed to execute commands on the local system.

/usr/lpp/sysback/.remote_cmds

Contains list of commands that can be executed remotely on the local system.

Related Information

The **sbcomp**, **sbuncomp**, **sbfwd** and **sbwrite** commands.

The **cfglocaccess** and **cfgremaccess** commands.

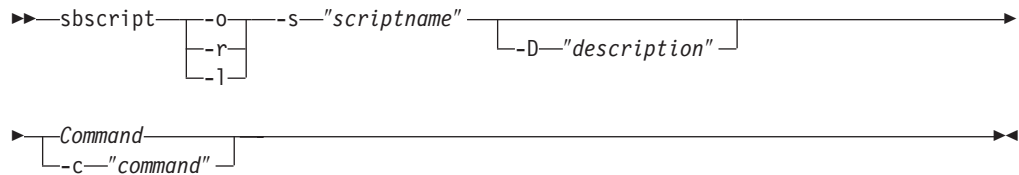
The AIX **backup** and **restore** commands.

sbscript

Purpose

Creates, updates, or removes a shell script containing the commands to execute.

Syntax



Description

Used to create, update, or remove a shell script containing one or more commands to execute. When creating or updating a script, you can type the command name or specify it using the **-c** flag.

Flags

-o Overwrites existing script name, if it exists.

-r Removes script name, if it exists.

-l Lists currently defined scripts.

-s "scriptname"
Name of the script to create, update, or remove.

-D "description"
Describes the shell script.

Command
Specifies the command or commands contained in the shell script. Separate the commands using spaces.

-c "command"
Specifies the command or commands contained in the shell script. Commands must be inside double quotation marks.

Examples

Use the following syntax to create a shell script called **system_backup** that will be a full system backup:

```
sbscript -s system_backup -D "System Backup -c "sysback -vf /dev/rmt0 sbvg vg01"
```

The following script is created:

```
#!/bin/ksh
#
# Description: System Backup
#
sysback -vf /dev/rmt0 sbvg vg02
rc=$?
exit $rc
```

A file in **/usr/lpp/sysback/scripts/.toc_script** is also updated. The format of the file is as follows:

Script Name Description

The file created from the above example would be as follows:

```
system_backup System Backup
```

To remove the script “wed.backup,” type:

```
sbscript -r -s /user/lpp/sysback/sbscripts/wed.backup
```

sbspboot

Purpose

Initiates a NIM Resource Network Boot of an SP node.

Syntax

```
➤—sbspboot—➤
  --d—"host"
  --n—"spot name"
  --c—"lppsource name"
  --c—"display"
```

Description

The **sbspboot** command is used to initiate a NIM Resource Network Boot of an SP node. Use this command instead of the Classic Network Boot method to ensure that the proper SP and PSSP specific scripts are executed. For more information about this command, see Chapter 13, “Network Boot/Installation Configuration”, on page 13-1.

This command must be initiated from the SP Control workstation.

The specified NIM **SPOT** and NIM **LPPSOURCE** entries must be the same as those specified when the client was added for network boot using the **mksbnetboot** command.

Flags

- h “host”**
Specifies the hostname of the SP node to be booted.
- n “spot name”**
Specifies the NIM **SPOT** resource to be used for the network boot process.
- l “lppsource name”**
Specifies the NIM **LPPSOURCE** resource to be used for post-installation processing.
- d “display”**
Specifies the hostname where a console window will be displayed during a prompted installation.

Examples

To initiate a network boot of an SP node called “bcn1e” using the NIM **SPOT** “spot_aix433” and the NIM **LPPSOURCE** “lppsource_aix433” and to open a console window on the host “lasher,” type:

```
sbspboot -h bcn1e -n spot_aix433 -l lppsource_aix433 -d lasher:0
```

Related Information

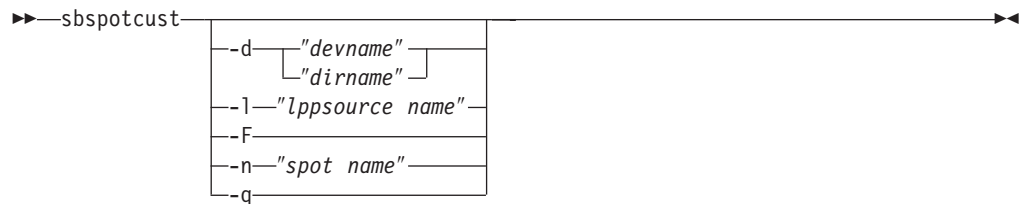
The **mksbnetboot** and **sbspotcust** commands.

sbspotcust

Purpose

Installs SysBack into a NIM **SPOT** resource.

Syntax



Description

When performing a NIM Resource Network Boot, SysBack must be installed into the NIM **SPOT** resource in order for the SysBack programs to be available during a network boot. The **sbspotcust** command reads the installation filesets from the specified input device or directory, copies them into the specified NIM **LPPSOURCE** directory, and installs them into the NIM **SPOT** from the NIM **LPPSOURCE** directory.

Note: You must run this command before adding a NIM Resource Network Boot client to ensure that the client's boot image contains the SysBack programs.

If you install or update the SysBack filesets contained in the NIM **SPOT** resource after the network boot client is added, you must update the network boot image used by the client using the **mksbnetboot** command.

Flags

-d "devname | dirname"

Specifies the input device name or directory name that contains the SysBack filesets.

-F Indicates to overwrite the same or newer version of SysBack in the NIM **SPOT** resource with the version contained on the installation media.

-l "lppsource name"

Specifies the NIM **LPPSOURCE** name to which the filesets will be copied.

-n "spot name"

Specifies the NIM **SPOT** name to which the filesets will be installed.

-q

Checks the specified spot to determine if a valid level of SysBack is installed. The **-n** flag is required.

Examples

1. To install SysBack to the NIM **SPOT** resource called "spot_433" from the /dev/cd0 device through the NIM **LPPSOURCE** called "lppsource_433", type:
sbspotcust -d /dev/cd0 -n spot_433 -l lppsource_433
2. To query the level of the spot in spot_433, type:

```
sbspotcust -q -n spot_433
```

Return Codes

- 0 Successful update of the specified spot
- 1 Spot does not contain the SysBack filesets.
- 2 Spot does not contain SysBack filesets.
- 3 Image location is invalid or does not exist.
- 4 Invalid spot or lpp_source specification.
- 5 Update of specified spot failed.

Related Information

The **mksbnetboot** command.

sbtsmdevice

Purpose

This command creates, modifies, or removes a TSM virtual device. For more information on this topic, please refer to “Create the TSM Virtual Device” on page 15-4.



-a:

```
--n "tsmvirdev" --s "tsmserver" --p "tsmpassord"
```

-c Option:

```
--n "tsmvirdev"
--s "tsmserver"
--p "tsmpassord"
```

-r Option:

```
--n "tsmvirdev"
```

Flags

- a** Specifies to add a TSM virtual device. This flag requires the use of the **-n** "tsmvirdev", **-s** "tsmserver", and **-p** "tsmpasswd" flags.
- c** Specifies to change or modify an existing TSM virtual device. This flag requires the use of one or more of the following flags: **-n** "tsmvirdev", **-s** "tsmserver", and **-p** "tsmpasswd"
- r** Indicates to remove the specified TSM virtual device. The flag requires the use of the **-n** "tsmvirdev" flag as well.
- l** Indicates to list all existing TSM virtual devices. No other flags are valid when this option is specified.
- n "tsmvirdev"**
Specifies the TSM virtual device name. This flag is required with the **-a**, and **-r** flags, and optional for the **-c** flag.
- s "tsmserver"**
Species the TSM server name stanza to use for contacting the TSM server located in the **/usr/tivoli/tsm/client/api/bin/dsm.sys** file.
- p "tsmpasswd"**
Specifies the TSM client node's password.

Files

The creates the file **/usr/lpp/tsm/dsm.opt.tsm#**.

Related Information

The `sbtsmlist`, `sbtsmnetcfg`, `mkvgback`, `mklvback`, `mkjfsback`, and `mkdirback` commands.

sbtsmlist

Purpose

This flag lists the current TSM management class bindings or backups stored in a TSM server. For more information on this topic, please refer to "Querying Backups and TSM Management Classes in Chapter 15.

►—sbtsmlist—

-l
-r

—n—"tsmvirdev"—►

-l:

-a
-o
-t "S V L F D"
-g "backupID"
-m

-r Option:

—g—"backupID"—

Flags

- r** Indicates to remove the TSM backup ID specified with the -g "backupID" flag.
- l** Indicates to list either the current TSM management class bindings or all backups stored in the TSM server as specified with the -n "tsmvirdev" flag. This option will list all active, inactive, and open backups for the backup type specified.

Note: Inactive backup versions are backups that are not the most recent backup for that backup type. There may be multiple inactive versions for each backup type. The number of inactive versions is determined by the backup copy group defined on the TSM server. For more information regarding active and inactive backup versioning, please refer to the *IBM Tivoli Storage Manager for AIX: Administrator's Guide* (GC32-0768) and the *IBM Tivoli Storage Manager for AIX: Administrator's Reference* (GC32-0769).

This flags requires the use of the -n flag. Also specifying the -m flag, or a choice of the -a, -o, and -t flags limits this output according to the function of the flags used. The -g "backupID" flag is not valid with this flag.

-n "tsmvirdev"

Specify the virtual device that represents the connection information for the TSM server as configured in the `/usr/tivoli/tsm/client/api/bin/dsm.sys` file. This flag is required.

--g "backupID"

Specify the unique object id for the backup stored in the TSM server. When specifying this option, the -l and -t flags are not valid with this flag.

-m Specify this flag to query the current management class bindings from within SysBack. The management class bindings are obtained from the server name

stanza in the **dsm.sys** file that is associated with the specified TSM virtual device. If no bindings are specified, the value "default" is returned. This flag is optional.

- a Active backup versions are the most recent copy of a backup type stored in the TSM server. There can be only one active version per backup type.
- o Open backups represent currently running backup processes, or partial backup images created by an abnormally terminated backup process.

Note: Open backups listed that do not correspond to an actively running backup process should be removed to avoid versioning once the next backup process for that backup type is initiated.

This flag is optional.

-t "S|V|F|L|D"

Specify the unique object id for the backup stored in the TSM server. When specifying this option, the **List Option** and **Backup Type** are ignored. The possible values for this flag are:

- SB: Full System (Installation Image) backup
- VG: Volume Group level backup
- FS: File System level backup
- LV: Logical Volume level backup
- FD: File / Directory level backup

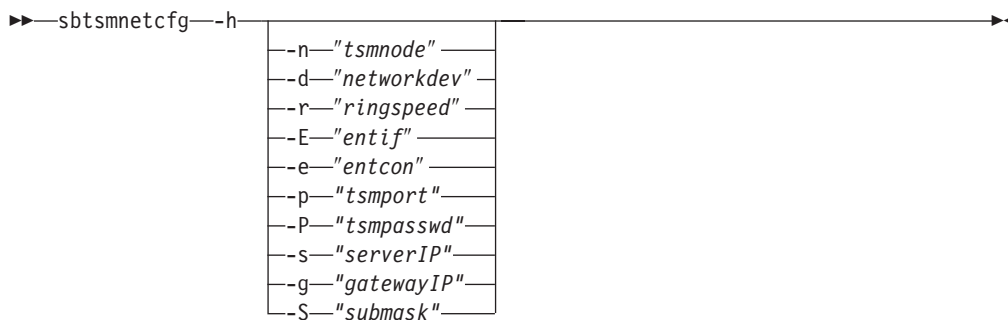
Related Information

The **sbtmdevice**, **sbtmnetcfg**, **mkvgback**, **mklvback**, **mkjfsback**, and **mkdirback** commands.

sbtsmnetcfg

Purpose

This command sets the TSM Network Client Install Defaults. For more informational this topic, please refer to “Configuring Network Boot Options for a TSM Bare Metal Recovery” on page 15-18



Flags

-h "hostname"

Specify the hostname of the system which was configured as a SysBack network boot client. The value for this field was populated by the input in the previous menu.

Note: The SysBack network boot client definition is based on the hostname of the client system. This may, or may not be, the same as the TSM client node name.

This flag is required.

-n "tsmnode"

Specify the TSM node name that will be used to connect to the TSM server for bare metal recovery. This flag is required.

-d "networkdev"

Specify the network device name to use for communications with the TSM server. For example: ent0. This flag is optional.

-r "ringspeed"

Specify the correct token-ring speed when a token-ring device specified in the **TSM Network Device** field. This field is optional.

--E "entif"

Specify either type of ethernet interface when an ethernet device is specified in the **TSM Network Device Name** field. For example: IEEE 802.3 This flag is optional.

-e "entcon"

Specify the connection type for the ethernet interface when an ethernet device is specified in the **TSM Network Device Name** field. For example: BNC. This flag is optional.

-p "tsmport"

Specify the TSM server port number that should be used to connect to the TSM server for bare metal recovery. This flag is optional.

-a "adminID"

Specify a TSM Admin ID that has client owner authority when the client node's password is unknown. When specifying a value in the field, you must also specify the Admin's password in the **Password** field rather than the client node password. This flag is optional.

-P "tsmpasswd"

Specify the TSM client password that is associated with the **TSM Client Node Name** value. If you do not know the password of the client node name, enter the password to administrative id created for this node which has client owner authority. In most cases, this was automatically created when you registered the node to the TSM server.

Note: If you do not know either password, you will have to log on to the TSM server as an administrator and issue the command: **update node your_nodename new_password**. Then enter that new password into this field.

This flag is optional.

-s "serverIP"

Specify the IP address that corresponds to the TCPServeraddress for the TSM server as defined in the file `/usr/tivoli/tsmservice/bin/dsmserv.opt` on the TSM server system. This flag is optional.

-g "gateway ID"

Specify the gateway address that this client system must go through in order to access the server system. If the client and the server are on the same subnet, it is recommended to re-enter the server's IP address here. This flag is optional.

-S "submask"

Specify the subnet mask, if required, for the client network interface to contact the installation server. This flag is optional.

Related Information

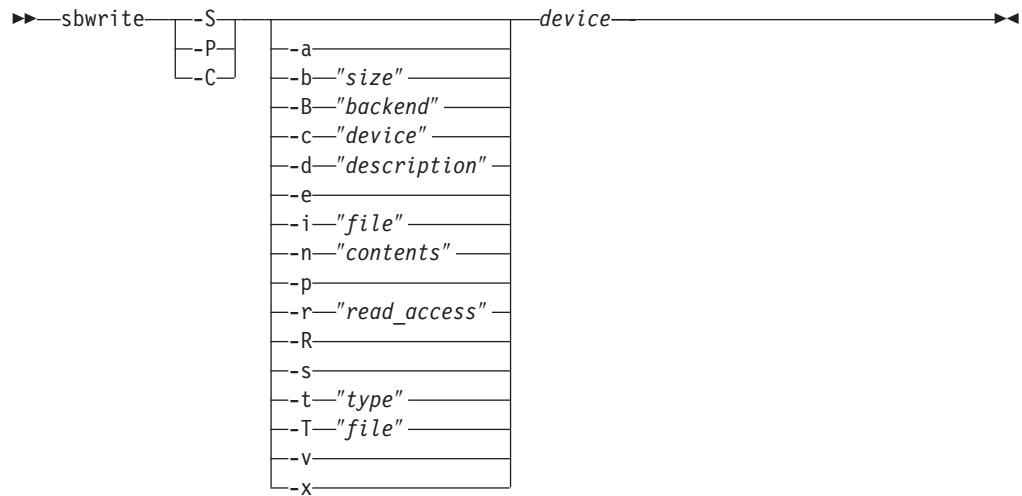
The `sbtsmdevice`, `sbtsmlist`, `mkvgback`, `mklvback`, `mkjfsback`, and `mkdirback` commands.

sbwrite

Purpose

Writes raw data to backup media.

Syntax



Description

The **sbwrite** command reads data from standard input, adds a backup header, optional file list, and LVM information, and writes to single or multiple devices either sequentially, in parallel, or by creating multiple copies. The device parameter can be either a single tape drive, multiple tape drives, a virtual device, or one or more disk image file names.

This command should be used only by the experienced user who wants to create backups without using the SMIT menus, and who is knowledgeable in the use of the **sbfwd** and **sbread** commands needed to restore data from backups made using this command.

The **sbwrite** command will write data only to backup devices or directories to which the local host and user have access, as defined by the or **cfgremaccess** commands. When **sbwrite** is executed locally, the access permissions are checked in the **.local_access** file. When executed by the **sbclient** command on a remote host, the remote host and user access permissions are checked in the **.remote_access** file.

Any command that produces a data stream to standard output can pipe that data stream to the **sbwrite** command. The **sbwrite** program then stores the data on the media, including the backup header, LVM information, and file list, if specified. The data can later be read from the backup media by the **sbread** program, which can then pipe the data stream to another command.

If the **-i file** option is specified, the data is read from the specified file, which can also be a logical volume name (preceded with the **/dev** prefix), instead of from standard input. If a dash (**-**) is specified for the output device name, the output is sent to standard output (*stdout*) instead of to a device or file.

Unless you are using a virtual device name for the device parameter, specify either the **-S** flag (indicating sequential backups), the **-P** flag (indicating parallel backups) or **-C** flag (indicating multi-copy backups). Each of the backup types are described in Chapter 21, “Virtual Devices”, on page 21-1.

The other options are used by the SysBack backup commands **mklvback**, **mkjfsback**, **mkdirback**, **mkvgback** and **sysback** to define the contents and format of the data contained in the backup but do not alter the way the data is read using the **sbread** command. For example, the **-t** “type”, **-n** “description” and **-d** “description” flags can be used to supply user and backup-specific information that will be stored in the header label on the backup.

The type parameter can be one of the following:

- s** System backup
- p** Power system backup
- v** Volume group backup
- L** Multi-logical volume backup
- F** Multi-filesystem backup
- l** Single logical volume backup
- f** Single filesystem backup
- d** file/directory backup
- o** other/unknown. This is the default if none is specified.

The “backend” parameter, specified with the **-B** flag, can be any single character that is used by SysBack to keep track of the format of the data in the data stream. For filesystem data, SysBack uses either “B” for the AIX **backup** command or “T” for the AIX **tar** command.

Data can be compressed using the **sbcomp** command before sending to the **sbwrite** command. If so, you should specify the **-p** flag to **sbwrite**, indicating that the data on the media is compressed, so you will know later to uncompress the data during a restore.

When **sbwrite** is executed remotely using the **sbclient** command, the hostname and user name of the actual user and host performing the command remotely are written to the backup header. When executed locally, the local user and hostname, if any, are included in the header.

To include a file list on the backup, supply the **-L** flag, followed by the name of the file containing the file list. This same option can be used to store any type of data. To read this data from the backup and display the results to stdout, use the **-L** flag of the **sbread** command. Likewise, to store additional information in the table of contents portion of the backup, use the **-T** flag with the name of the file containing the table of contents data. The table of contents can be read from the backup using the **-T** flag of the **sbread** command.

Flags

- a** Indicates the device is an auto-loader. User is not prompted to change volumes, but the reading continues automatically when the next volume is inserted.

- b **"size"**
Specifies the buffer size in K-bytes (1024-bytes). Changing this value either increases or decreases the amount of data that is written to the output device at one time. Some devices with small buffers might require you to reduce this value, while other devices with very large buffers can benefit from increased performance by increasing this value. If you are unsure, use the default value (64 Kbytes).
- B **"backend"**
Specifies any single character representing the command used to create the data stream.
- c **"termdev"**
If the backup contains multiple tape volumes, the volume prompt is sent to the "termdev" device (such as /dev/tty0).
- C
Indicates the backup should be performed with a multi-copy write policy. The same data is written to all specified devices. If used, multiple device names must also be provided.
- d **"description"**
A custom description to be included in the backup header. Up to 60 characters can be used. This information will be placed in the backup header. If the description includes spaces, the entire description must be enclosed in double quotation marks ("").
- e
Indicates all devices (if tape) should be rewound upon completion. The default is to not rewind at end.
- i **"file"**
Indicates the name of a file or logical volume (with /dev prefix) that contains the data to be written using **sbwrite**. If not specified, **sbwrite** reads the data from standard input.
- l **"level"**
Specifies a single character representing the incremental backup level. SysBack backups use a digit between 0 and 9.
- L **"file"**
Indicates the file list, included in the file specified by the "file" parameter, should be included on the backup.
- n **"contents"**
If supplied, "contents" describes the contents of the backup (such as the volume group name or directory name). Up to 128 characters can be included. This information is placed in the backup header. If contents includes spaces, the entire contents must be enclosed in double quotation marks ("").
- p
Indicates the data being sent to **sbwrite** is packed (compressed). This is informational only and does not alter the input data. Specifying the **-p** flag with **sbwrite** causes the "Packed" field in the backup header to show "Y" when reading the header with the **"sbread -H"** command.
- P
Indicates the backup should be performed with a parallel write-policy, so all specified devices should be written to synchronously. If specified, multiple device names must be supplied.

- r **user=[u | a]**
Specifies user read permission when writing to a disk image file. “u” indicates only this user can read the file. “a” indicates any user can read the file.
- r **host=[h | a]**
Specifies host read permission when writing to a disk image file. “h” indicates only this host can read the file. “a” indicates any host can read the file.
- R
Indicates the file list and table of contents file, if any, are to be removed after the command is complete.
- S
Indicates the backup should be performed using a sequential write-policy. In this case, the backup is written to the first device. When full, the next device in the list is used for the second volume. Only when all specified devices are full are you prompted to change the media in all drives. This option should be used by default when only one device name is specified.
- t “type”
Indicates the type of backup being performed. Valid types are **d** (file/directory), **l** (raw logical volume), **v** (volume group), **0 through 9** (incremental filesystem *level*) or **o** (other).
- T “file”
Indicates the table of contents, included in the file specified by the “file” parameter, should be included on the backup.
- v Indicates summary header information should be displayed before writing the data. This information is sent to standard error.
- x Indicates the progress indicator should be displayed as the files are being written. If -x is used, the command sending the data to **sbwrite** should not update the screen.

Examples

1. To create a backup of all files using the AIX **backup** command, compressing the data with **sbcomp** and formatting the output to 2 parallel *auto-loading* tape drives, *rmt0* and *rmt1*, type:

```
find / -print | backup -ivqf- | sbcomp | sbwrite -aP \
    -td rmt0 rmt1
```
2. To write the file **/home/myfile** sequentially to the virtual device *vdev1*, including a backup description and displaying the progress indicator while writing, type:

```
cat /home/myfile | sbwrite -x -td -n"Transaction log" \
    vdev1
```
3. To write the file list contained in the file **/tmp/filelist** to a backup of the **/home** directory, writing multiple copies to drives */dev/rmt1*, */dev/rmt2*, and */dev/rmt3*, type:

```
find /home -print | backup -ivqf- | sbwrite -Cv -td \
    -n"/home" -L/tmp/filelist rmt1 rmt2 rmt3
```

Files

/usr/lpp/sysback/.remote_access

Contains list of hosts and users that are allowed to execute commands on the local system.

`/usr/lpp/sysback/.remote_cmds`

Contains list of commands that can be remotely executed on the local system.

Related Information

The `sbclient`, `sbcomp`, `sbuncomp`, `sbfwd` and `sbread` commands.

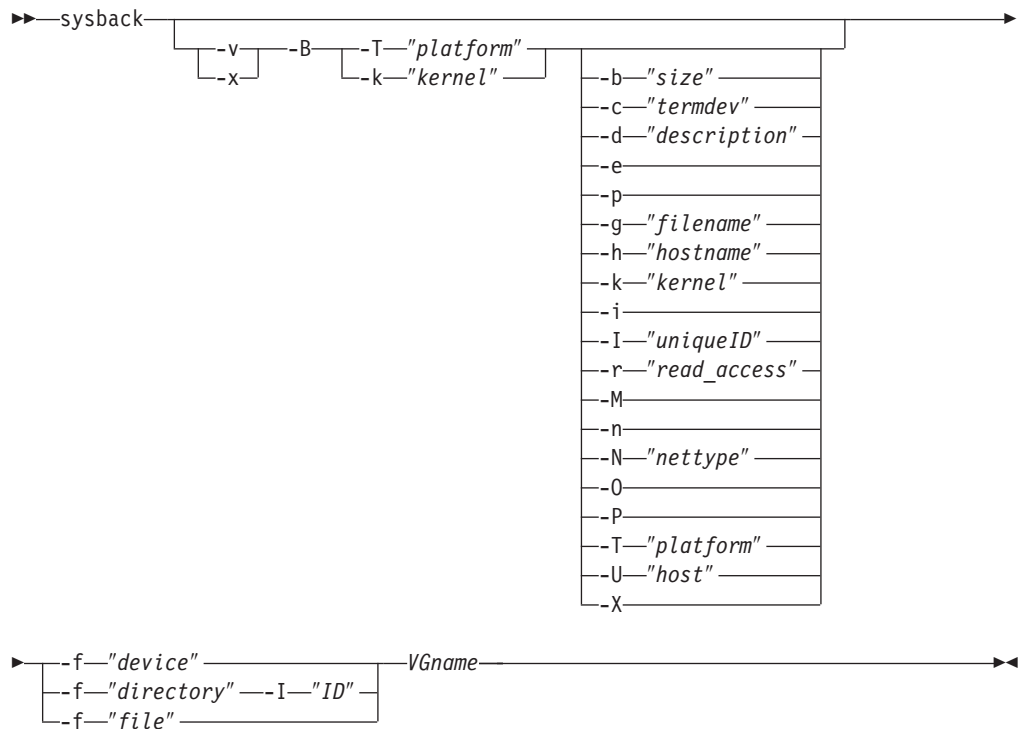
The AIX `backup` command.

sysback

Purpose

Backs up the entire system or specific volume groups for use in a system installation.

Syntax



Description

The **sysback** command is used to create a backup of the operating system (rootvg volume group) and optionally other volume groups on the system. This backup can be used to completely reinstall a system to its original state or to install a new system from the customized image. It can also be used to recreate or restore select files, directories, filesystems, logical volumes, or volume groups on an already active system. If backing up to a tape device, the tape will be bootable and will include the installation programs needed to install from the customized backup.

The backup can be performed to a tape drive, virtual device, or disk image file. When specifying a disk image file, you can enter the full pathname of the file to create or overwrite. When doing so, the filename must begin with the prefix "SB." to indicate the file is a SysBack system backup. You can also specify only the backup directory and a unique ID. When doing so, a filename will be constructed for you. Refer to "Backups to Disk Image Files" on page 2-6 for information on the filename created. If you are creating a file and a file by the same name already exists, specify the **-O** option to overwrite the existing file.

The backup can also be performed to a remote device, virtual device, or disk image file. If *Remote Services* has been configured on both the local and server system using the **cfgremsvs** command, and you have defined a backup device on

the server for use by this system using the **cfgremaccess** command, then you can also select a hostname using the **-h** option. The backup is then written to the device or filename on the specified server, provided the server has enabled this system access to the specified device or directory.

The backup can also be performed as a “pull” backup to enable central management of backups. The machine that “pulls” the backup is called the “initiator,” while the machine that is backed up is called the “backup system.” The machine that receives the backup data is called the “destination system.”

The initiator is the machine where the **mkdirback** command is issued. The backup system is referenced in the command syntax by the **-U “host”** flag. The data destination system is referenced by the **-h “host flag”**.

When only the **-U “host”** flag is specified, the **-f “device”** flag refers to a device on the initiator system. In this case, the backup destination and the initiator are the same system. This is known as a “two-way pull backup.”

When the **-U “host”** and **-h “host”** flags are specified, the **-f “device”** flag refers to a device on the host specified by the **-h “host”** flag. In this case, the backup destination and the initiator are different systems. This is known as a “three-way pull backup.”

Remote Services must be configured, using the **cfgremsvs** command, on all of the machines involved in the backup operation, the initiator, the backup system, and the data destination machines. The backup destination machine must have the Server Options of Remote Services configured to allow the backup system machine to send its data to devices on the backup destination machine. You can do this with the **Add or Change Client Host Access to this Server** option or the **cfgremaccess** command.

The backup system machine must have the Client Options of Remote Services configured to specify the backup destination machine as a backup host. You can do this with the **Add or Change List of Remote Backup Servers** option or the **cfgremserver** command.

The backup system must also configure Remote Command Access to allow the initiator machine to pull the backup.

To include network support in the boot images of the tape, specify the **-N nettype** option. This enables a network installation to be performed after booting a system from this tape. This flag is valid only when a tape device is used. Valid network types are *ethernet*, *token ring* or *FDDI*. You can also specify a device name (such as */dev/ent0*, */dev/tok0* or */dev/fddi0*) for the nettype parameter.

The **sysback** command calls the **mkvginfo** program to generate information on volume groups, logical volumes, filesystems, paging space, and physical volumes. This information can be used later to recreate the system or any of the included volume groups to its original state. The **mkvginfo** command creates a temporary file that is placed in the table of contents on the backup, or you can create a customized file using the **mkvginfo** and **editlvminfo** commands and include it instead on the backup by also specifying the **-g “filename”** option to this command. Files, or files within directories, that are specified in the exclude list are not backed up with this command. See the **chexcludelist** command for information on creating exclude lists.

Cloning Systems: A System backup created on one machine can be installed on another machine with a different processor, platform type, or other system devices. However, the machine being backed up must have installed all of the device support for the destination platform type, processor type, and other required devices.

If the platform or kernel type differs between the system being backed up and the system that is installed from the backup, the boot image on the tape must be created for use on the destination system. This is accomplished by specifying the **-T** “platform” and **-k** “kernel” options.

The following platform types are currently supported with the **-T** flag:

chrp	Common Hardware Reference Platform
rs6k	“Classic” RISC System/6000 Uni or Multi-processor (AIX 4.2+)
rs6ksmp	Multiprocessor RISC System/6000 (AIX 4.1 only)
rspc	PCI-based (PC) RISC System/6000

The following kernel types are supported with the **-k** flag:

up	Uniprocessor (single processor)
mp	Multiprocessor

Power System Backup: If the **-P** flag is specified, a *power* system backup is created. The power backup differs from the regular system backup in that all filesystem data is backed up as raw logical volume data. This can increase the performance of the backup and restoration of the data considerably but imposes certain limitations on the system installation and restoration of data from the backup:

- No filesystem attributes or mount point can be changed during a system installation from this backup.
- The logical volume name, logical volume size, and stripe size attributes of the logical volumes cannot be changed during a system installation from this backup.
- Only entire logical volumes or filesystems can be restored from the backup, and only if the logical volume and filesystem, if applicable, are currently inactive. It is not possible to restore individual files or directories from the backup.
- The entire filesystem is backed up as raw logical volume data. This might result in longer backup and restore time for filesystems that were only partially full.

When you create a system backup, **sysback** performs the following functions:

1. Executes the user-created **Pre-backup Script**. Appendix D, “Creating Scripts for Customizing the System Backup and Install Process”, on page D-1 describes how to create this script. This script can perform any function required by the user prior to the backup process.
2. If you are backing up to a tape device, the block size of the tape drive is temporarily changed to 512-byte blocks, if necessary. This ensures that the installation programs are able to read from the media. The block size is changed back to its original value before the volume group files are placed on the media.
3. Generates an LVM information file, using the **mkvginfo** command, that will contain the information for all volume groups, logical volumes, and filesystems.

This file is used by the installation process to regenerate the same volume group configuration. This step is ignored if the **-g** "filename" option was specified.

4. Places boot image and installation programs on the tape in separate images. This enables the installation process to be accessed by booting from the tape. This step is ignored if the backup media is not a tape.
5. The data for each filesystem and logical volume is written to the backup media, each in a separate backup image.
6. Executes the user-created **Post-backup Script**. This script can perform any functions required by the user after the completion of the backup, but prior to the rewinding and verifying of the backup format. Appendix D, "Creating Scripts for Customizing the System Backup and Install Process", on page D-1 provides information on creating this script.

Flags

-b "size"

Specifies the buffer size in K-bytes (1024-bytes). Changing this value either increases or decreases the amount of data that is written to the output device at one time. Some devices with small buffers might require you to reduce this value, while other devices with very large buffers can benefit from increased performance by increasing this value. If you are unsure, use the default value (64 Kbytes). The value specified must be a multiple of the tape block size.

-B

Indicates that only boot images are to be created on the tape. This flag is invalid unless a tape device is specified. When this flag is used, all other options, with the exception of the device name and platform type, are ignored.

-c "termdev"

If the backup contains multiple tape volumes, the volume prompt is sent to the "termdev" device (such as /dev/tty0).

-d "description"

A custom description to be included in the backup header. Up to 60 characters can be used. This information will be placed in the backup header. If the description includes spaces, the entire description must be enclosed in double quotation marks ("").

- e** Forwards to the end of the last SysBack backup on the tape. Used when stacking backup images on the same tape.

-f "device, file or directory"

Specifies the output device name, filename, or directory for the backup. The specified output option can be on the local system or server (if **-h** option provided). The device name can be a tape drive or virtual device name. If a directory is specified, you must also specify an ID using the **-I** flag.

-g "filename"

Indicates the name of a LVM information file previously created and customized for this backup. Refer to the **mkvginfo** and **editlvminfo** commands.

-h "hostname"

Name of the remote backup server host to receive the backup data (such as the data destination host). This is the host that provides the backup device specified by the **-f** flag.

- i Indicates to dynamically create a backup file IDD when writing backups to a disk image file. This flag supersedes the **-I "ID"** flag and is useful when scheduling a backup to disk image file.
- I **"ID"**
This option is used only if a directory is specified as the output device. The ID is included in the filename created to make it unique from other disk image file backups. If a backup in the same directory with this ID already exists, specify the **-O** flag to overwrite the previous backup.
- k **"kernel"**
When backing up to tape, indicates the kernel type of the machine that will be booting from the tape. The default is to create a bootable tape for the current kernel type.
- M
Retains physical partition mapping, by default, when logical volumes are recreated from this backup. Unless the logical volumes were originally created using physical partition maps, it is generally recommended that they not be recreated using the same partitions, as this would preserve fragmentation that develops over time as logical volumes and filesystems are expanded. You can specify whether or not partition mapping is used before the logical volumes are recreated.
- n
Indicates that the backup is to be placed at the current tape location without rewinding the tape. Only if the tape is positioned at the start of tape are boot images placed on the tape. If the tape is *not* positioned at the start of the tape, the backup is appended to the prior backup and can later be restored from by entering a *backup sequence number* with the **sysrestore** command.
- N **"nettype"**
Specifies that device support for the indicated network type should be included on the tape boot images.
- O
Indicates that, if a filename was specified as the output device, and the filename already exists, that the new backup will overwrite the previous file.
- P
Indicates that the data should be packed before being written to the media. This typically reduces size of backup between 25% and 40%. For increased performance, do not use this option when backing up to a device that provides hardware data compression.
- r **user=[u | a]**
Specifies user read permission when writing to a disk image file. **"u"** indicates only this user can read the file. **"a"** indicates any user can read the file.
- r **host=[h | a]**
Specifies host read permission when writing to a disk image file. **"h"** indicates only this host can read the file. **"a"** indicates any host can read the file.
- T **"platform"**
When writing to tape, specifies the platform type for which the boot image will be created. The default is to create boot images for the current platform type.
- U **"host"**
Name of the host to be backed up (such as the backup system).
- v Lists the files as they are backed up. This flag cannot be used with the **-x** flag.

- x Displays the progress indicator as the backup is being performed for each volume group. This flag cannot be used with the -v flag.
- X Excludes all non-JFS (journaled filesystem) logical volumes, or “raw” logical volumes, from the backup.

Examples

1. To generate a backup of the root volume group only, to the tape drive */dev/rmt0*, displaying the progress indicator, type:

```
sysback -nxf rmt0
```

Because the -n option is specified, the tape needs to be rewound. If the tape is already at the start of media, the resulting backup will be on a bootable tape. If not, the backup will be appended to the prior data.
2. To generate a backup of the root volume group and the *uservg* and *datavg* volume groups, using virtual device *vdev2*, and making the backup bootable on a multiprocessor RSPC machine, enter:

```
sysback -f vdev2 -T rspc -k mp uservg datavg
```
3. To generate a compressed (packed) backup of the *rootvg* and *uservg* volume groups to the disk image file */usr/lpp/sysback/images/all/SB.venus.04281007* on host *mars*, listing files as they are backed up, enter:

```
sysback -pvh mars -f \  
/usr/lpp/sysback/images/all/SB.venus.04281007 uservg
```
4. To initiate a pull backup of the */home* filesystem on host *lasher*, from host *sysback1*, and send the data to *rmt1* of the host *sysback1*, type the following from *sysback1*:

```
sysback -U lasher -f /dev/rmt1 /home
```
5. To initiate a pull backup of the */home* filesystem on host *lasher*, from host *sysback1*, and send the data to *rmt1* of the host *shappy*, type the following command from *sysback1*:

```
sysback -U lasher -h shappy -f /dev/rmt1 /home
```

Related Information

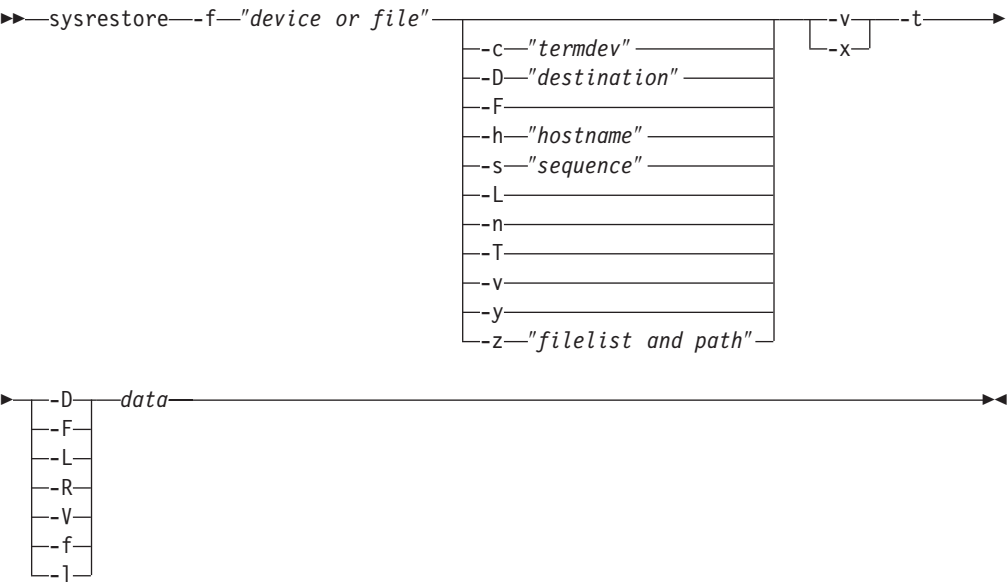
The **mkvginfo**, **cfgremsvs**, **cfgremaccess**, **cfgremrootaccess**, and **chexcludelist** commands.

sysrestore

Purpose

Restores or verifies data on any SysBack backup or lists backup type or contents.

Syntax



Description

The **sysrestore** command is used to either verify or restore data from any type of backup created with SysBack. This command can also be used to list the backup type or the contents of the backup.

The command can be performed from a remote device, virtual device, or disk image file. If *Remote Services* has been configured on both the local and server system using the **cfgremsvs** command, and you have defined a backup device on the server for use by this system using the **cfgremaccess** command, then you can also select a hostname using the **-h** option. The command can then access devices or files on the server, provided the server has enabled this system access to the specified device or directory.

When specifying a local or remote filename, do not include the file extension (*.TOC* or *.lvname*) added by the SysBack **backup** command. The **sysrestore** command automatically reads the specified data from the file or files with the appropriate extension.

Different types of data can be verified or restored from different types of backups:

Backup type	Verify/Restore types
System backup	volume groups, filesystems, logical volumes, directories, files
Power backup	volume groups, filesystems, logical volumes
Filesystem	filesystems, directories, files

Logical volume	logical volumes
File/Directory	directories, files

When restoring a volume group, all logical volume and filesystem data within the volume group is restored. When restoring directories, all files within the directories are restored as well, even if the files are contained in different filesystems.

The *data* argument can be a list of either volume groups, filesystems, logical volumes, directories, or files, depending on the type of data to be listed, verified, or restored (as indicated by the **-t** flag).

The **-t** option must be specified to indicate the type of data to verify or restore. For instance, a volume group backup can contain multiple volume groups, filesystems, and raw logical volumes. To restore two specific filesystems from the backup, you must specify the **-tF** option, and the data argument at the end of the backup must contain the mount points of the filesystems to restore. To restore only a specific directory from a backup, regardless of the backup type, you must specify the **-tD** option, and the *data* argument must be the directory or directories to restore.

To verify the backup by reading the data, specify the **-V** flag. When specified, the data on the backup is read but no data is restored. You still need to specify the type and data you want to verify. For example, to verify only a couple of raw logical volumes on a volume group backup, specify the **-V** flag, the **-tL** option, and the names of the logical volumes to verify as the data argument. To verify the entire contents of a System backup, you must specify the **-V** flag, the **-tV** flag, and the names of all volume groups to verify.

The **-L** flag is used to list the contents of the backup, depending on the type specified with the **-t** flag. The following table indicates the data list that is created with the **-L** flag, based on the type:

type (-t)	Produces list of:
V	Volume groups
L	Logical volumes
F	Filesystems
D	Directories
R	Regular files
f	Directories and regular files
l	Filesystems and logical volumes

The **-T** flag queries the type of backup and returns a single character as follows:

S	System backup
P	Power system backup
V	Volume group backup
F	Filesystem backup
L	Logical volume backup
D	File/directory Backup

The **-i** “sequence” option is used to specify which backup to verify or restore when multiple backups are stacked onto the same tape or series of tapes. If this flag is specified, and the value is greater than 1, the tape or tapes will be automatically forwarded to the beginning of the desired backup before verifying or restoring data.

The **-F** flag must be specified to allow restoration of system directories or files that are not ordinarily replaceable. Restoring files to these directories can have adverse affect on the system or even cause a system failure, and should be used with extreme caution. Those directories are:

- /
- /dev
- /etc/vg
- /etc/objrepos
- /usr
- /usr/lib
- /usr/lib/objrepos

Specifying a new destination: The **-D** “destination” option indicates that the data should be restored to the new destination.

When you restore from a file/directory backup, the files or directories will be restored relative to the specified destination but will include the full path of the original files. For instance, if a file **/home/tony/file1** is restored to destination **/tmp**, the resulting file would be **/tmp/home/tony/file1**.

When you restore from a system, volume group or filesystem backup, the files are restored to the destination directory, but the filename does not contain the prior mount point of the filesystem. For instance, if files are restored from the **/home** filesystem to the **/tmp** destination, a file previously called **/home/tony/file1** will be restored as **/tmp/tony/file1**.

To restore logical volume data to a new location, specify a new logical volume name. The specified logical volume name cannot be currently active.

Incremental Restores: The **-y** flag must be specified to enable restoration of incremental data. To restore the entire contents of an incremental backup, this flag must be specified. The resulting filesystems will contain the same files as it did at the time the backup was created. This can, in some cases, require files to be re-removed from the filesystem that were deleted prior to the incremental backup level being performed.

If the **-y** flag is not specified, you can restore only select files and directories from an incremental backup. Refer to “Understanding Incremental Backups” on page 4-1 for important details on restoring data incrementally.

Notes:

1. This command is not intended for restoring an entire AIX operating system. The only way to restore the entire system is to reinstall from the system backup. Refer to Chapter 12, “System Installation and Maintenance”, on page 12-1.
2. When specifying the files to restore, SysBack supports the use of BRE (Basic Regular Expression) wild cards to restore a wildcard match of files. The files and the wildcard must be enclosed in double quotation marks (") to avoid

expansion by the user's shell. For example, `"/home/j*"` would indicate to restore all directories and files that start with `/home/j` such as `/home/john` or `/home/jenn`.

Flags

-c "termdev"

If the backup contains multiple tape volumes, the volume prompt is sent to the "termdev" device (such as `/dev/tty0`). If the **-h** hostname option is specified, this flag indicates the device on the remote host.

-D "destination"

Indicates that files should be restored to the directory specified by the "destination" parameter or the logical volume data should be restored to the logical volume specified by the "destination" parameter, rather than to their original locations.

-f "device or file"

Specifies the input device name or filename of the backup. The specified option can be on the local system or on a backup server (if **-h** option provided). The device name can be a tape drive or virtual device name.

-F Enables the restoration of system files or directories otherwise non-replaceable.

-h "hostname"

Hostname of backup server to which the remote backup device is attached.

-H

Creates a detailed usage listing on the screen for this command. When specified, no other action will be performed.

-i "sequence"

Specifies the backup to list, verify, or restore on a tape or series of tapes containing multiple (stacked) backups. The default is "1", or the first backup on the media.

-L

This flag causes the command to read and display the items on the backup of the specified type (indicated by the **-t** flag).

-n

Indicates the tape is already positioned at the beginning of the backup to read. When this flag is supplied, the **-i** sequence option is ignored.

-t "type"

Indicates the type of data to be listed, verified, or restored.

-T

Reads the backup header and displays a single character representing the backup type. No other action is performed.

-v Displays the file names as they are either verified or restored. This flag has no affect when verifying or restoring logical volumes. Do not specify this flag if the **-x** flag is used.

-V

Indicates that the backup contents should be verified, rather than restored. Only items of the specified type (indicated by the **-t** flag) are verified.

-x Displays the progress indicator, including the approximate size and time to read the entire contents of the media and the amount completed. Do not specify this flag if the **-v** flag is used.

- y Indicates that an incremental restore can be performed. This flag is required if the backup is an incremental backup and restoring other than specific files or directories.
- z **"filelist and path"**
Specifies the path and name of a file containing a list of files to restore.

Return Codes

The **sysrestore** command returns a value, which can be queried with the \$? shell variable, indicating the success or failure of the process as follows:

- 0 The process was completely successful.
- 1 The process terminated due to an unknown error.
- 2 The process terminated because there was an error writing the backup data to disk.
- 3 There were read errors when reading the backup data from the backup media. The failure resulted in loss of some data and possibly termination of the restore, depending on the number of read errors and how SysBack is configured to handle them.
- 4 There were sync errors when reading the backup data from the backup media. The failure resulted in loss of some data and possibly termination of the restore, depending on the number of sync errors and how SysBack is configured to handle them.
- 5 The process completed successfully, however there were non-fatal errors when writing one or more files to disk.

Examples

1. To restore the **/tmp** directory and its contents from the disk image backup **/usr/lpp/sysback/bf/VG.localhost.06230300**, displaying the progress indicator instead of the file list as the files are read, type:

```
sysrestore -x -tD \
-f/usr/lpp/sysback/bf/VG.localhost.06230300 /tmp
```
2. To restore the files **/data/file1** and **/data/file2** from a backup on virtual device **vdev1**, type:

```
sysrestore -tR -fvdev1 /data/file1 /data/file2
```
3. To list all files and directories included in the backup on device **/dev/rmt0** attached to host *neptune*, enter:

```
sysrestore -L -tf -h neptune -f rmt0
```
4. To show the names of all logical volumes and filesystems included on the backup on tape device **/dev/rmt1**, type:

```
sysrestore -L -tl -frmt1
```
1. To verify the uservg volume group on the backup on device **/dev/rmt0**, showing the files as they are read, type:

```
sysrestore -Vv -tV -f rmt0 uservg
```
2. To determine the backup type of the second backup on the tape, type:

```
sysrestore -T -f rmt0 -i2
```

Related Information

The **sysback**, **mkdirback**, **mklvback**, **mkjfsback** and **mkvgback** commands.

Appendix B. Booting a System for SysBack Installation or Maintenance

This appendix provides the specific step-by-step instructions for booting a system to the SysBack Installation and Maintenance menu, used to install a system from a SysBack system backup.

The instructions for booting the system to the Installation and Maintenance menus differ depending on whether the system is booted from a bootable tape or from a network boot server, and also differ depending on the type of the machine to be booted. Instructions are provided for each of the following machine types:

- Common Hardware Reference Platform (uni or multiprocessor)
- Microchannel-based RISC System/6000 (uniprocessor)
- Microchannel-based RISC System/6000 SMP (multiprocessor)
- PCI-based (RSPC) RISC System/6000 (uni or multiprocessor)
- Scalable POWERparallel (SP) Node (uniprocessor)
- Scalable POWERparallel (SP) Node (multiprocessor)

If an error occurs during a network or tape boot, a value might appear in the system LED panel. On many PCI-based systems, the LED panel is optional but makes troubleshooting a network boot much easier. Refer to Appendix C, “LEDS”, on page C-1 for a detailed explanation of the LED codes used in SysBack. For LED values that are not listed in Appendix E, refer to the AIX documentation.

There are three steps to boot a system:

1. Initiate the boot process.
2. Initiate the network boot (for systems booted from the network).
3. Complete the boot.

Initiating the boot process

The following sections describe how to begin the boot process for the different types of systems.

Common Hardware Reference Platform (uni or multi-processor)

The CHRP systems are actually PCI-based and the boot process is identical to other PCI-based systems. To boot these systems, refer to the instructions in “PCI-based (RSPC) RISC System/6000 (uni or multi-processor)” on page B-3.

Microchannel-based RISC System/6000 (uniprocessor)

You can boot a microchannel-based RISC System/6000 system in one of two ways: from a SysBack system backup tape or from a network boot server.

Booting from a SysBack system backup tape

To boot the system using a system backup tape:

1. Insert the system backup tape in the drive.
2. Turn the system key to the SERVICE position.

3. Turn on the system or press the yellow button twice.
4. Continue with “Completing the Boot Process” on page B-4

Booting from a network boot server

Use these instructions to obtain the BOOTP screen:

1. Turn the system key to the SECURE position.
2. Turn on the power to the system. After a short sequence of numbers, the LED displays 200.
3. Turn the key to the SERVICE position and press the yellow reset button once.
4. If the LED value displays 260, 261, or 262, and the BOOTP Main menu is displayed on the screen, continue with “Initiating the Network Boot” on page B-4.

If the above instructions *did not* work, you need to boot from an IPLROM Emulation Diskette:

1. Insert the *IPLROM Emulation Diskette*.
2. Turn the system key to the SERVICE position.
3. Turn on the power to the system or press the yellow reset button twice.
4. Continue with “Initiating the Network Boot” on page B-4.

Microchannel-based RISC System/6000 SMP (multiprocessor)

You can boot a microchannel-based RISC System/6000 system in one of two ways: from a SysBack system backup tape or from a network boot server.

Booting from a SysBack system backup tape

1. Insert the system backup tape.
2. Power off the system.
3. Turn the system key to the SERVICE position.
4. Press Enter until the “>” prompt appears.
5. Type sbb and press Enter to view the STAND-BY.
6. Select option 1, **Set Flags**.
7. Select option 2, **Autoservice IPL**. Make sure this value is set to “enable”. If so, press “n”. If it is currently set to “disable”, press “y” to change it.
8. Select option 6, **Fast IPL**. Make sure this value is set to “enable.” If it is, press “n”. If it is currently set to “disable,” select “y” to change it.
9. Type x to return to the “>” prompt.
10. Type x again to clear the screen.
11. Power on the system.
12. Continue with “Completing the Boot Process” on page B-4.

Booting from a network boot server

1. Power off the system.
2. Turn the system key to the SERVICE position.
3. Press Enter until the “>” prompt appears.
4. Type sbb and press Enter to view the STAND-BY.
5. Select option 1, **Set Flags**.
6. Select option 2, **Autoservice IPL**. Make sure this value is set to “enable.” If it is, press “n”. If it is currently set to “disable,” press “y” to change it.

7. Select option 6, **Fast IPL**. Make sure this value is set to “enable”. If it is, press “n”. If it is currently set to “disable,” select “y” to change it.
8. Type x to return to the “>” prompt.
9. Type x again to clear the screen.
10. Power on the system.
11. From the MAINTENANCE menu, select option 6, **SYSTEM BOOT**.
12. Select option 1, **BOOT FROM NETWORK**.
13. Press Enter at the language prompt for English. The BOOTP MAIN menu is displayed.
14. Continue with “Initiating the Network Boot” on page B-4.

PCI-based (RSPC) RISC System/6000 (uni or multi-processor)

For PCI-based RISC System/6000 (RSPC) machines, booting from tape or network is accomplished through the *System Management Services* (SMS). System Management Services is included in the firmware of most models and is loaded from diskette on other older models. System Management Services can be executed using a graphical, icon-based, interface, or an ASCII, text-based, emulation. The steps provided below are for the ASCII (text-based) interface.

Booting from a SysBack system backup tape, CD, or DVD

1. If the RSPC model does not include SMS in the firmware, insert the *System Management Services* Diskette.
2. Power on the system.
3. When the first screen appears (a picture is displayed and icons begin showing at the bottom of the screen), press “F1” if you have a graphics console or “1” if it is an ASCII console.
4. From the System Management Services menu, select **Boot** and press Enter.
5. Select the desired boot device (tape, CD, DVD) to be the first boot device but placing a “1” next to it.
6. Select the option to “save” your selection.
7. Press the ESC key three times. The system should begin booting after the third escape iteration.
8. Continue with “Completing the Boot Process” on page B-4.

Booting from a network boot server

1. If the RSPC model does not include SMS in the firmware, insert the *System Management Services* Diskette.
2. Power on the system.
3. When the first screen appears (a picture is displayed and icons begin showing at the bottom of the screen), press “F1” if you have a graphics console or “1” if it is an ASCII console.
4. From the System Management Services menu, select **Utilities** and press Enter.
5. Select **Remote Initial Program Load Setup (RIPL)**.
6. Select **Set Address**.
7. Fill out all fields, including the *server IP address*, *gateway address (the client’s gateway)* and *subnet mask (the client’s subnet mask)*.
8. Select the option to “save” your selection.
9. Press the ESC key three times. This returns you to the main **System Management Services (SMS)** menu.
10. Select **Boot**.

11. Select the network adapter to boot from which to boot by placing a " 1" next to the entry.
12. Select the option to "save" your selection.
13. Press the ESC key three times. The system will begin to boot and the bootp and tftp process should begin.
14. Continue with "Completing the Boot Process".

Initiating the Network Boot

From the BOOTP Main menu, use these steps to initiate a network boot:

1. Select option 1, *Select BOOT1, Select BOOT (Startup) Device*.
2. Do not select the **Default Boot (Startup) Device** option, but rather the appropriate network adapter and connector that applies to your node. Make sure you select the appropriate interface option (BNC, DIX or built-in ethernet, 4 or 16 MB token-ring data rate).
3. Change the *Client address*, *Server address* and *Gateway address* as needed by selecting the number corresponding to each entry field. Then, enter the IP address for each. The IP address entries requires leading zeros in each portion of the IP address (i.e. "005.001.001.024"). The *Gateway address* may be set to the Server's IP address if both systems are in the same segments.
4. When all entries are complete, type "99" to return to the *MAIN MENU*.
5. Select the option to *Exit Main Menu and Start System (BOOT)*. The option number will vary.
6. On SP Systems, put the key in NORMAL mode using the *Node Front Panel*. Press Enter once more to continue.
7. Continue with the "Completing the Boot Process".

Completing the Boot Process

If booting from a network boot server and the client is configured for no-prompt install, the installation proceeds without any user prompts. Refer to the section **Set Network Install Client Defaults** in Chapter 8, "Remote Services", on page 8-1 for details on the configuration of a no-prompt install.

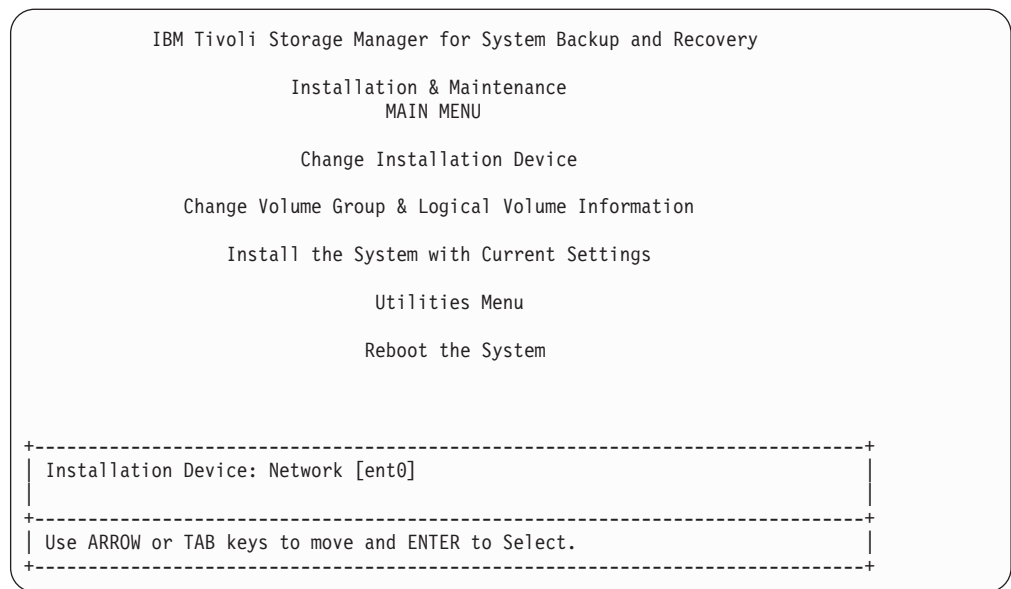
Unless this is a no-prompt install, the following prompt will appear on the screen:

***** Please define the System Console *****

Type 1 at this terminal and press <Enter>
if you want this display to be the System Console.

The above example is for an ASCII terminal. Note that the prompt Type 1 is Press F1 for graphical displays. If the console is an ASCII terminal, press 1 and Enter. If the console is a graphic display, press F1 and Enter.

After a short time, the following SysBack Installation and Maintenance screen is displayed:



The detailed instructions for using the options on this menu are provided in Chapter 12, “System Installation and Maintenance”, on page 12-1 and Chapter 11, “Changing the Volume Group, Logical Volume and Filesystem Attributes”, on page 11-1.

Troubleshooting a Network Boot

To boot from the network, a server must have first been configured to provide a network boot image to this client. Those steps are outlined in Chapter 13, “Network Boot/Installation Configuration”, on page 13-1 under **Create a Network Boot Image** and **Configure a Network Boot Client**.

The system hardware must either be BOOTP enabled, or you must have created an *IPLROM Emulation Diskette* to perform a network boot. All PCI and SMP systems are BOOTP enabled, but some older Microchannel-based (non-SMP) systems are not. If you are unable to obtain the BOOTP *MAIN MENU* using the prior steps, your system might not be BOOTP enabled.

Determining the Network Adapter Hardware Address

Configuring the network boot client sometimes requires the *network adapter hardware address* of the client. The steps to obtain the network adapter hardware address of the client differ depending on the type of platform:

1. **Microchannel-based/SP systems:** The network adapter address is determined by performing the first steps in a network boot. Follow the steps below for initiating a network boot on this platform. When selecting the network adapter to boot from, the hardware address of the adapter is displayed.
2. **PCI-based (RSPC) systems:** The network adapter address may be displayed using *System Management Services* (SMS). SMS is included in the firmware of some rspc models, and is loaded from diskette on other models. To determine the hardware address, follow these steps:
 - a. If the RSPC model does not include SMS in the firmware, insert the *System Management Services Diskette*.
 - b. Power on the system.

- c. When the first screen appears (a picture is displayed and icons begin showing at the bottom of the screen), press F4.
- d. From the System Management Services menu, select **Utilities** and press Enter.
- e. Select the *Tools* icon.
- f. Select **Remote Initial Program Load Setup**.
- g. Select **Adapters**.
- h. Select the network adapter the machine will boot from.
- i. Record the *Adapter Hardware Address*.

Appendix C. LEDS

This chapter contains a list of the system LED codes that might appear when you boot or install from a SysBack System Backup. Many of the LED codes are for information only and usually occur when there is no system console available; others indicate an error in the boot or installation process.

Many of the LED codes appear only during a *no-prompt installation*. This is because there may not be a system console attached and the LED is used to provide information to the user on the progress of the installation, or because an error occurred that requires user intervention.

The LED codes below are those that are provided by SysBack. Any other codes that appear are not part of the SysBack product but normally represent a system software or hardware problem. If the LED code is not listed here, refer to your AIX software diagnostics documentation for details.

000 Failed to identify the system type during a tape boot

The *bootinfo -B* command failed due to device support missing from the boot image that is required to support the client system's hardware. The problem usually is caused by missing SCSI device support. You need to recreate the boot tape from a system containing all device support required for the system to be installed.

c04 An unrecoverable error occurred during a no-prompt installation

A message has been displayed on the system console. Press Enter on the console to display the detailed error message.

c06 Failed to identify the system type during a network boot

The *bootinfo -B* command failed due to device support missing from the boot image that is required to support the client system's hardware. The boot server is likely missing device support for either the token-ring, ethernet or FDDI adapter. You need to install the appropriate device support on the server system, reboot the server, and remake the network boot image for the client.

c21 Unable to configure logical network device during a network boot

The *ifconfig* command failed. Report the problem to your network service organization.

c31 Prompting user to select a system console

c32 User selected a graphical display as a console device

c33 User selected an ASCII display as a console device

c40 Installation data is being extracted from the install media during a no-prompt install

c43 Error restoring the AIX install programs during a tape boot

Either the tape media is defective, the tape drive is defective, or the boot tape is incomplete. Create another boot tape and try booting from tape again.

c45 Failed to configure a system console

The *cfgcon* command failed because of missing device support for either the graphic adapter or standard I/O slot for ASCII monitors. You must install the appropriate device support on the system from which the backup tape was made, or install the appropriate device support on the network boot server, reboot the server, and remake the network boot image for the client.

c46 Normal installation processing during a no-prompt install

c47 Unable to create a PVID on a disk

This normally indicates a hard disk failure. If you are installing on the disk for the first time, check and reformat, if necessary, the disk in diagnostics and retry the installation.

c48 Prompting user for input during a no-prompt install

An error has occurred during a no-prompt installation. This LED is used to alert the user to the message displayed on the system console. The installation process has defaulted to prompt mode. Press Enter on the console to re-display the specific error message, then use the normal installation menus on the screen to correct the problem and begin the installation.

c50 The rootvg volume group is being created during a no-prompt install

c52 Changing from boot (RAM) to restored rootvg file systems during a no-prompt install

200 The system key is in secure mode when booting

If booting from network, turn the key to service mode and press the reset key. If booting from tape, power off, turn the key to service, and power on.

260, 261 or 262

The *BOOTP* menus have been invoked

The system is to be booted from the network and the *BOOTP* menus have been invoked. If they are not displayed, press Enter on the console.

510 Configuring base system devices during a tape boot

511 then blank screen

Console configured but messages cannot be displayed

The *cfgcon* successfully configured a system console device; however, the console messages are not displayed because of missing or incorrect device support for the graphic adapter. You must install the appropriate device support on the system from which the backup tape was made, or install the appropriate device support on the network boot server, reboot the server, and remake the network boot image for the client.

512 Configuring additional system devices during a tape boot

513 Restoring installation files from tape during a tape boot

600 Starting a network boot

602 Configuring base system devices during a network boot

603 Configuration of base system devices failed during a network boot

There is likely device support missing from the boot image which is required to support the client system's bus, I/O or disk hardware. You need to install the appropriate device support on the server system, reboot the server, and remake the network boot image for the client.

604 Configuring the boot network

605 Invalid network boot device provided

The boot server is likely missing device support for either the token-ring, ethernet, or FDDI adapter. You need to install the appropriate device support on the server system, reboot the server, and remake the network boot image for the client.

606 Configuring the boot network.

608 Copying network boot information file from boot server

609 Failed to copy network boot information from boot server

The **tftp** command failed to tftp the file **/tftp/Client Hostname.sbin** from the boot server. One of the following usually apply:

1. The file does not have read permissions for all users.
2. The file does not exist.
3. An **/etc/tftpaccess.ctl** file exists on the boot server but does not provide access to the **/usr/lpp/sysback/netinst/boot** directory.
4. On a PCI-based system, you cannot use the leading zero's for any of the IP address in the SMS Menu. Even though the first **tftp** command works, the second one run will fail.

Rebuild the network boot image on the server and add the network boot client, making sure all values are correct.

610 NFS mount of /usr fleshiest from the server is hanging

The **/etc/exports** file does not have permissions for the client to mount **/usr**. Type **exportfs** on the server and look for the line starting with **"/usr"**. Make sure the client hostname is included on the line and that **/usr** is exported with root permission.

Example of output:

```
/usr -ro,root=node1,node2
```

In the above example, only node1 and node2 are exported. Add the network boot client again and verify that all the values are correct for the server's IP address, the gateway, and the subnet mask for the client.

611 NFS mount of /usr fleshiest from the server failed

This often means that **/usr fleshiest** was not exported to the client (see LED 610). There are known problems in AIX Version 4.1 that will affect SysBack network boots. These problems are fixed in the following file set levels:

- bos.adt.prof 4.1.4.5
- bos.rte.libc 4.1.4.5
- bos.net.nfs.client 4.1.4.4
- bos.sysmgt.quota 4.1.3.1
- bos.net.tcp.client 4.1.4.4

Make sure the above filesets are at this level or later. If updating the filesets, reboot the server, then remake the network boot image on the server.

613 Configuration of gateway failed during network configuration

The route command failed to add the gateway address provided. Report the problem to your network service organization.

Appendix D. Creating Scripts for Customizing the System Backup and Install Process

To add additional flexibility and automation to the backup and installation process for requirements specific to a particular customer environment, SysBack can call user-created shell scripts, if they exist, before and after the system backup and after completion of the installation process when installing from a system backup.

These shell scripts can perform any function required and are executed with root user authority. The following are examples of functions you might want to perform:

Pre-backup functions:

- Remove all temporary files from the system to prevent unnecessary backup time and space.
- Send a message to all users that a backup is being performed.
- Automatically log users off the system.
- Shutdown the network daemons or disable tty ports to prevent user logins.

Post-backup functions:

- Restart network daemons and enable tty ports to allow users to log on.
- Send a message to a user or users that the backup is complete.

Post-install functions:

- Enable a shell for the install user to perform maintenance tasks.
- Remove unwanted configuration data from the system (i.e. user IDs and passwords). This is needed when cloning systems from a single backup image.

Script Names

During installation of System Backup & Recovery for AIX, the `/usr/lpp/sysback/scripts` directory is created. This directory has read and write permissions only for the root user. Do not give any other user permission to add or change the scripts in this directory, because all scripts are executed with root user authority.

You can create four scripts, which can contain any function, in this directory. The scripts must be owned by root and must have execute permissions.

The SysBack system backup looks for the following scripts and executes them before installation if they exist:

`/usr/lpp/sysback/scripts/fsback.pre`

This script is executed when the **System Backup** option is selected from the SMIT menus or when the **sysback** command is executed. The script is executed before any other function is performed. Any environment variables exported before the backup is run are available to this script. In addition, the following variables will be defined:

DEVICE Name of tape devices, virtual device, or backup image file.

HOSTNAME Name of remote backup server, if any.

/usr/lpp/sysback/scripts/fsback.post

This script is executed at the end of the SMIT **System Backup** option or at the end of the **sysback** command. It is executed after all data is backed up for the root and other volume groups (if selected), but *before* the backup format is verified. Because the tape is left positioned at the end of the backup, this script might contain commands to append to the tape additional information that is not part of the system backup. Any environment variables exported before the backup is run are available to this script. In addition, the following variables are defined:

DEVICE Name of tape devices, virtual device, or backup image file.

HOSTNAME Name of remote backup server, if any.

The SysBack installation process looks for the following scripts and executes them at the end of installation if they exist:

/usr/lpp/sysback/scripts/install.pre

This script must exist on the system where the system backup tape was created or on the network boot server. It is restored and executed before the installation menus appear. The following variable will be defined:

BOOTDEV Name of the boot device (i.e. "rmt0" for tape or "ent0" for ethernet adapter).

/usr/lpp/sysback/scripts/install.postroot

This script must exist on the system where the system backup was created. After all files are restored onto the newly installed system, this script exists on the new system. It is executed immediately after the root volume group data is restored, before any additional processing, such as recreating the boot logical volume or restoring the non-rootvg volume groups. Refer to "Post-Installation Scripts" on page D-3 for additional information.

/usr/lpp/sysback/scripts/install.post

This script must exist on the system where the system backup was created. After all files are restored onto the newly installed system, this script exists on the new system. It is executed as the last step in the installation process, just before the system reboot. Refer to "Post-Installation Scripts" on page D-3 for additional information.

Note: The scripts must have execute permissions or they will be ignored. To set the execute permissions, type the following after creating the scripts:

```
chmod u+x filename
```

(where "filename" is the name of the script file)

If any of the scripts return a non-zero error code or contain syntax errors, the backup or installation process alerts you and asks you to press Enter before continuing. The remainder of the process will then continue as usual. Within the scripts, checks should be made to ensure they are performing as planned, and the scripts should exit with a non-zero return code if they fail to perform their desired function. A "1" return code is sent by executing the **exit 1** command from within the script.

Post-Installation Scripts

The post-installation scripts can perform any commands available to the restored system. They can also perform remote commands, but only to the server from which the system was installed. There are several environment variables available to the post-installation scripts. They are as follows:

CLIENTIP	IP address of the restored system, if installed from a network install server. Note that this must be used in place of the HOSTNAME variable since the hostname is not defined at this time.
DEVICE	Local tape drive names such as <code>"/dev/rmt0"</code> or remote tape drive name or filename.
GATEIP	IP address of the gateway machine, if any.
NETDEV	Device name of the network adapter (<code>ent*</code> , <code>tok*</code> , or <code>fddi*</code>), if booted or installed from a network installation server.
POLICY	Indicates the sequential or parallel backup policy (S/P) if multiple local tape devices are used.
REL	AIX Release level of the restored system
REMOTE	Set to <code>"1"</code> if the installation was performed from a network install server. Otherwise, this variable is not set. If set, the <code>/etc/hosts</code> file on the client contains the <code>"instserver"</code> alias, which can be used with either the sbclient or other TCP commands to access the install server.
SERVERIP	IP address of the installation server, if any. You cannot use the server's hostname because it is not defined at this time.
SUBNET	Subnet mask, if any.
VER	AIX Version of the restored system.
VGINFO	Filename of the temporary volume group information file. See the <code>"mkvginfo"</code> on page A-49 for the contents.

You can use these environment variables to access the local or remote installation devices.

Sample Scripts

There are a few sample scripts in the `/usr/lpp/sysback/scripts` directory. These can be modified as desired and enabled by changing the name of the sample script to the appropriate file name described above.

Note: The sample scripts provided are available to assist users in creating their own custom backup and installation scripts and are not supported by IBM.

The following sample scripts are contained in this directory:

fsback.pre_killusers

This sample script, when enabled, informs all users on the system that a system backup will start in 5 minutes. It resends the message each minute until the 5 minutes expire and then ends all user processes, except for the root user's. The system backup continues only after the user processes have been terminated.

To enable this script, change the name to **fsback.pre**.

install.postroot_hwmigrate

This sample script allows you to install a system backup created on a different system onto a new machine, even though the new machine has different device support software requirements. The new system must be booted from media that contains the required base device support, but the source system from where the backup was created does need to have the software support pre-installed.

To boot the new system from the media with the required base device support, place an *AIX Version 4 Installation CD* in the drive of the new system during the installation process. After the rootvg volume group data is restored, the additional required device support is automatically added to the new system from the CD-ROM.

To enable this script, change the name to **install.postroot**.

install.post_rmnet

This script automatically removes any network configuration from the system at the end of the installation process. This is necessary when installing multiple systems from the same system backup to prevent multiple machines from existing on the network with the same network configuration.

This script also prevents SysBack from being removed from the system at the end of the installation process.

If this script is not enabled, and a system is installed from a system backup created from a different machine, you are prompted to select whether or not to remove the network configuration and the SysBack product.

To enable this script, change the name to **install.post**.

Appendix E. Device/System-Specific Information

This chapter provides various notes and tips for using SysBack with various types of devices, networks, or systems. The devices described in this chapter are not the full list of devices supported by SysBack. The information provided here is specific to devices or systems commonly used with SysBack, in which the performance or usability might be impacted by the configuration of SysBack, the device, or the system itself.

IBM 7208 8mm Tape Drives

All of the 7208 8mm tape drive models use a physical hardware blocking factor of 1024 bytes. This does not prevent the tape drive block size from being set to 512 bytes, but doing so causes the remaining 512 bytes of each physical block to go unused. Therefore, half of the tape capacity, and up to half of the backup performance, is lost if the tape block size is set to 512 bytes.

For best performance, the **tape block size should be set to 1024 bytes**, or any multiple thereof.

IBM 3490, Magstar®, DLT and LTO Tape Drives

These are very high performance tape drives and contain a very large data buffer. To achieve their highest throughput, send data to the tape drive's buffer in very large blocks. To do so, set the **Buffer Size** to 256 Kbytes when performing any SysBack backup. Change the block size of the tape drive to either 0 or 262144 (256 Kbytes) using the **Change Tape Drive Characteristics** option. Doing so helps ensure the drive continues streaming data without having to stop and wait for additional data from the system. You can set the buffer size to a higher value as long as the value is a multiple of the tape drive's block size.

Note: Examples of drives in these categories are the IBM 3490, 3590, 3570, 3575, 7205, 7337, 3580, 3581, 3583, 3584., and third party DLT drives. You should check with your vendor to determine if your drive benefits from using large blocks.

Note that increased performance of the tape drive does not necessarily result in faster backups if the data being backed up cannot be read at the same rate the tape drive is writing. In many cases, reading fragmented data from a filesystem on even the fastest disk drive can have trouble keeping up with the write performance of these tape drives. To achieve the best performance, read performance of the disk drives can be increased by keeping data contiguous on the disk and striping data across multiple disks to spread the I/O workload evenly across multiple devices. The settings and recommendations are not specific to SysBack. They are attributes of the device driver and affect other commands that use the drives, such as tar, or mksysb.

Also, make sure the tape drive **Autoload** feature is set to "no." You can change this feature using the **Change Tape Drive Characteristics** option. If this option is set to "yes," the loader changes tapes automatically, making the entire set of tapes appear like a single tape to SysBack. Instead, turn this option off so that SysBack handles the tape changes, placing a new volume label on each tape. It is absolutely

imperative that this be done for certain IBM devices that use the Atape.driver to ensure proper SysBack function. Failure to do so can render your data unrecoverable.

Any tapes previously created with “autoload=yes” should be tested for the ability to recover them. They can only be recovered by resetting “autoload=yes” since the tape was made that way. The command to set this attribute is: Also, for IBM devices that have the device driver option “use random mode to emulate auto”, this must also be set to ‘no’. To determine if your device driver has this setting, issue the command:

```
chdev -l rmtX -a autoload=no
```

where X represents your tape drive number.

Also, for IBM devices that have the device driver option “use random mode to emulate auto”, this must also be set to ‘no’. To determine if your device driver has this setting, issue the command:

```
lsattr -El rmtX
```

where X represents your tape drive number. To change this setting, issue the command:

```
chdev -l rmtX -a emulate_auto=no
```

where X represents your tape drive number.

Other Tape Drives

Any tape drive that is recognized by AIX should be usable by SysBack, although no support can be guaranteed. Most tape drives have at least a 64 Kbyte buffer, which is the default buffer size that SysBack uses. If you are using a tape drive that does not have a large buffer, usually resulting in a “*write: I/O error*” or “*illegal parameter*” messages, you might need to reduce the buffer size value SysBack uses each time a backup is performed. Try using “32” (Kbytes) as the next value, then “16,” and so on. If the error continues, either the tape drive or tape media is defective, or it is not supported by AIX or SysBack.

IBM 7331 8mm Tape Library

If the 7331 8mm Tape Library is installed with 2 tape drives, SysBack backups usually achieve twice the performance of a single 8mm tape drive when configured as described in this section.

To configure SysBack and the 7331 library for the best performance, create a SysBack parallel virtual device containing both tape drives in the unit. Then set the 7331 to “Split Sequential” mode. This allows SysBack to “stripe” the data across both tape drives, achieving twice the performance, while allowing the 7331 to change the tapes in each drive as the backup reaches the end of volume.

When in Split-Sequential mode, the 7331 assigns the first, or top, 10 tapes in the magazine to the top tape drive and the bottom 10 tapes in the magazine to the bottom tape drive. Note that the SCSI connection to the 7331 library itself is not used by SysBack, only the SCSI connection to the tape drives themselves.

IBM 7332 4mm Tape Library

The 7332 is a low-cost tape drive providing fast 4mm tape write performance, while allowing unattended operation of a tape autoloader. When configured for use with SysBack, either 4 internal or 12 external tapes can be written to sequentially without user intervention.

To do so, create a sequential virtual device containing the single 4mm tape drive and indicate that an autoloader is used. Any backups performed to this tape drive automatically span across as many tape cartridges are in the magazine without user intervention.

Other Tape Libraries or Autoloaders

Most tape libraries, or autoloaders, that have a “sequential mode” can be used with SysBack. “Sequential Mode” indicates that the tape loader itself automatically inserts a new cartridge each time a cartridge is ejected from the drive. The tape cartridges are usually inserted in sequential order, depending on their location in the unit, but some loaders allow the user to select the order in which the tapes will be used.

To use SysBack with an autoloader, create a sequential virtual device containing the tape drive (not the loader itself), and indicate in the virtual device configuration that an autoloader is used. Then, set the autoloader to sequential mode.

By not using any device-specific loader controls, SysBack can work with virtually any tape loader set in sequential mode. SysBack does not control the loader in any way. Instead, SysBack rewinds and ejects the current tape from the drive any time a read or write operation reaches end of tape and waits for the loader to insert the next volume. Upon doing so, the backup continues automatically without user intervention.

Because libraries or loaders can differ, SysBack cannot claim to support every loader, as the sequential operation is the function of the loader and not of SysBack. It is therefore up to the user to perform the steps to properly configure the loader and verify the proper operation of the sequential mode as described above.

For information related to enabling SysBack to execute your own customer scripts to manipulate the robotic mechanism of your library, please refer to “End of Tape (EOT) Processing Options” on page 16-23.

IBM 7133 Serial Storage Architecture (SSA) disk subsystem

The serial storage architecture provides a high-speed interconnection technology for SSA disk drives. The drives and cables are hot-plugable, which enables a disk drive to be replaced while the unit is operational. Also, the location within the loop is transparent to AIX, enabling a disk not currently in use to change locations without affecting the operation of the system.

Because AIX does not keep track of the physical location of the disk drive, it is not possible for SysBack to record and later reference a disk by its physical location. Instead, SysBack keeps track of the physical volume ID, which is unique to each individual disk drive. When you recreate a volume group on the same physical disks as they were previously installed, all disks are recognized and automatically added to the volume group. However, when you clone systems or replace a drive,

the disk or disks appear to be missing. You can use the **Edit volume group and logical volume attributes** option to re-select the drives for each volume group.

IBM 7135 RAIDiant Array

The IBM 7135 is not a supported boot device by AIX. During the SysBack system installation process, AIX recognizes the disks as “Other SCSI Disk”. AIX cannot, however, create a volume group on the disks at this time. The 7135 should be powered off or disconnected when using SysBack to install the system.

When the installation is complete and before rebooting the system in normal mode, power on the 7135. Each of the 7135 disks is then recognized as a “7135 Disk Array Device”, assuming the 7135 device support was installed on the system. You can then recreate and restore volume groups on the 7135 disks using the SysBack system backup.

When AIX is installed, it “walks the bus,” configuring all disks in the order in which they appear. Powering off the 7135 during installation of the rootvg ensures that the internal disk drives, onto which the *rootvg* volume group is installed, are named with the first hdisk names (e.g., *hdisk0*).

IBM 7137 and Other RAID Devices

RAID storage units have a number of unique features that vary depending upon the actual RAID box and have an impact on the use of SysBack. RAID boxes provide fault tolerance in case of a disk failure (except for RAID-0, which is simply a form of disk striping). Most implementations of RAID use RAID-5 or RAID-1, which provide fault tolerance for a disk failure.

Before a RAID box can be used, it must be configured. This often includes choosing the RAID level, number of LUNs (known as “hdisks” to AIX), size, and other characteristics. Creating and configuring the LUNs is done in various ways: through software on the RS/6000 such as for the IBM 7135, through a keypad on the RAID box such as for the IBM 7137, or through other means such as a terminal attached to the RAID box, switch settings, and so on. Only after the LUNs are configured in the system do the “hdisks” become available for use in AIX volume groups.

Some RAID devices, including the 7137, are recognized by AIX without the need to configure any software on the system; however, the disk descriptions show as “Other SCSI disks”. In most cases, as with the 7137, the disks can be used by AIX with no further software configuration. Because no special software configuration is required, they can be recognized by the SysBack installation process and can be included in any volume group, including the *rootvg* volume group.

If the RAID device requires special device drivers or software customization before they can be used, they are either unrecognized or unusable during the SysBack installation process. If this is the case, power off the unit during the installation process to ensure that the remaining system disks receive the first available “hdisk” names. After the *rootvg* volume group is installed on other supported disks, you can power on the RAID unit before rebooting the system in normal mode. At that time, assuming the RAID software support is installed, the RAID disks can then be configured into the system. Additional volume groups can be recreated and restored from the SysBack system backup onto the RAID disks.

Appendix F. Accessibility

Accessibility features help users with physical disabilities, such as restricted mobility or limited vision, to use software products successfully. The major accessibility features in this product enable users to do the following:

- Use assistive technologies, such as screen-reader software and digital speech synthesizer, to hear what is displayed on the screen via the operating system command line interface available for this product. Consult the product documentation of the assistive technology for details on using those technologies with this product.
- Operate specific or equivalent features using only the keyboard

In addition, the product documentation was modified to include features to aid accessibility:

- All documentation is available in a convertible PDF format to give the maximum opportunity for users to apply screen-reader software.
- Standard shortcut and accelerator keys are used by the product and are documented by the operating system. Refer to the documentation provided by your operating system for more information.

Appendix G. Notices

This information was developed for products and services offered in the U.S.A. IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service. IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chrome, Minato-ku
Tokyo 106, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you. This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
Information Enabling Requests
Dept. M13
5600 Cottle Road
San Jose, CA 95193-0001
U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee. The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrates programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. You may copy, modify, and distribute these sample programs in any form without payment to IBM for the purposes of developing, using, marketing, or distributing application programs conforming to IBM's application programming interfaces.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

Trademarks

The following terms are trademarks of International Business Machines Corporation in the United States or other countries or both:

- AIX
- @server
- Enterprise Storage Server
- IBM
- IBMLink
- Magstar
- POWERparallel
- pSeries
- Redbooks
- RISC System/6000
- RS/6000
- Scalable POWERParallel Systems
- SP
- SysBack
- Tivoli

EMC is a registered trademark of EMC Corporation

Other company, product, and service names may be trademarks or service marks of others.



Printed in U.S.A.

GC32-9076-01

